



INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

Itziar Alkorta Idiakez
Cristina Argelich Comelles
Maria Cristina Berenguer Albaladejo
Yolanda Bustos Moreno
Maria Raquel Evangelio Llorca
Beatriz Extremera Fernández
Pedro José Femenía López
María Remedios Guilabert Vidal
María Jorqui Azofra
Raúl Lafuente Sánchez
Pedro José López Mas
Raquel Luquin Bergareche
Andrés Marín Salmerón
Luz Martínez Velencoso
Lucía Molina Martínez
Óscar Monje Balmaseda
Esther Monterroso Casado
Juan Antonio Moreno Martínez
Carmen Muñoz García
Alberto Muñoz Villarreal
Íñigo Navarro Mendizábal
Manuel Ortiz Fernández
Miquel Peguera Poch
Antonio Rubí Puig
Alberto Tapia Hermida

**INTELIGENCIA ARTIFICIAL
Y DERECHO DE DAÑOS:
CUESTIONES ACTUALES**

Acorde al Reglamento (UE) 2024/1689

COLECCIÓN
DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

DIRECTOR
JUAN ANTONIO MORENO MARTÍNEZ
Catedrático de Derecho Civil de la Universidad de Alicante

COMITÉ EDITORIAL
ISIDORO BLANCO CORDERO
Catedrático de Derecho Penal (Universidad de Alicante)

FERNANDO CARBAJO GASCÓN
Catedrático de Derecho Mercantil (Universidad de Salamanca)

MANUEL DESANTES REAL
Catedrático de Derecho internacional privado (Universidad de Alicante)

JULIAN LÓPEZ RICHART
Profesor Titular de Derecho Civil (Universidad de Alicante)

JUAN JOSÉ MARÍN LÓPEZ
Catedrático de Derecho Civil (Universidad Castilla-La Mancha)

JAVIER PLAZA PENADÉS
Catedrático de Derecho Civil (Universidad de Valencia)

JULIÁN VALERO TORRIJOS
Catedrático de Derecho Administrativo (Universidad de Murcia)

RAQUEL XALABARDER PLANTADA
Catedrática de Propiedad Intelectual (Universitat Oberta de Catalunya)

INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

**MORENO MARTÍNEZ, J.A.
FEMENÍA LÓPEZ, P.J.**
(Coordinadores)

ITZIAR ALKORTA IDIAKEZ	LUZ MARTÍNEZ VELENCOSO
CRISTINA ARGELICH COMELLES	LUCÍA MOLINA MARTÍNEZ
MARIA CRISTINA BERENGUER ALBALADEJO	ÓSCAR MONJE BALMASEDA
YOLANDA BUSTOS MORENO	ESTHER MONTERROSO CASADO
MARIA RAQUEL EVANGELIO LLORCA	JUAN ANTONIO MORENO MARTÍNEZ
BEATRIZ EXTREMERA FERNÁNDEZ	CARMEN MUÑOZ GARCÍA
PEDRO JOSÉ FEMENÍA LÓPEZ	ALBERTO MUÑOZ VILLARREAL
MARÍA REMEDIOS GUILABERT VIDAL	ÍÑIGO NAVARRO MENDIZÁBAL
MARÍA JORQUI AZOFRA	MANUEL ORTIZ FERNÁNDEZ
RAÚL LAFUENTE SÁNCHEZ	MIQUEL PEGUERA POCH
PEDRO JOSÉ LÓPEZ MAS	ANTONIO RUBÍ PUIG
RAQUEL LUQUIN BERGARECHE	ALBERTO TAPIA HERMIDA
ANDRÉS MARÍN SALMERÓN	

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web www.conlicencia.com o por teléfono en el 917021970/932720407.

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial.
Para mayor información, véase www.dykinson.com/quienes_somos

Este trabajo se enmarca en el Proyecto I+D+i (Referencia: PID2020-116185GB-I00) del Ministerio de Ciencia e Innovación: “La irrupción de la inteligencia artificial en el Derecho de Daños y su adaptación a las nuevas tecnologías”, siendo investigadores principales los profesores Juan Antonio Moreno Martínez y Pedro José Femenía López.

© Copyright by
Los autores
Madrid

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69
e-mail: info@dykinson.com
<http://www.dykinson.es>
<http://www.dykinson.com>

ISBN: 978-84-1070-708-5
Depósito Legal: M-25437-2024
DOI: <https://doi.org/10.14679/3532>

ISBN electrónico: 978-84-1122-801-5

Preimpresión por:
Besing Servicios Gráficos S.L.
e-mail: besingsg@gmail.com

Índice

La discriminación algorítmica en el sector sanitario	1
ITZIAR ALKORTA IDIAKEZ	
1. INTRODUCCIÓN.....	1
2. CASOS DE DISCRIMINACIÓN ALGORÍTMICA EN EL SECTOR SANITARIO	3
3. APLICABILIDAD LA NORMATIVA ANTIDISCRIMINATORIA EN MATERIA DE DISCRIMINACIÓN ALGORÍTMICA	6
3.1. Normativa antidiscriminatoria	7
3.2. Limitaciones de la eficacia horizontal	9
3.3. La prueba del daño moral	10
3.4. Litigación colectiva	13
4. APLICABILIDAD DE LA NORMATIVA SECTORIAL DE LA IA.....	15
4.1. Principios y requisitos aplicables a la seguridad de los productos sanitarios con IA	15
4.2. La falta de transparencia en las decisiones automatizadas.....	17
4.3. El problema de la calidad de los conjuntos de datos	20
4.4. La responsabilidad por daños morales causados por la IA	24
5. CONCLUSIONES	26
La armonización del tratamiento legal de la responsabilidad civil contractual y extracontractual del metaverso con la regulación europea sobre plataformas en línea	31
CRISTINA ARGELICH COMELLES	
1. CONSIDERACIONES INICIALES ACERCA DEL METAVERSO Y LA RESPONSABILIDAD CIVIL.....	31
2. IDENTIDAD DIGITAL DEL RESPONSABLE CIVIL Y PROPIEDAD DE LOS ACTIVOS DIGITALES PATRIMONIALES.....	33

3.	EL RÉGIMEN DE RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE LA PLATAFORMA Y DEL USUARIO PROFESIONAL EN EL ORDENAMIENTO JURÍDICO EUROPEO	35
3.1.	La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad civil contractual: hacia un sistema de responsabilidad civil objetiva por pérdida o desprogramación de un activo digital y por discriminación algorítmica	39
3.2.	La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad extracontractual por los daños causados en las plataformas del Metaverso	43
4.	REFLEXIONES PROSPECTIVAS SOBRE LA RESPONSABILIDAD CIVIL CONTRACTUAL Y EXTRA CONTRACTUAL: EL INFORME ESPAÑOL PARA LA COMISIÓN EUROPEA EN MATERIA DE CONTRATACIÓN CON INTELIGENCIA ARTIFICIAL	44
	BIBLIOGRAFÍA	46
	Transparencia y explicabilidad para prevenir la discriminación de los sistemas de inteligencia artificial: la interacción entre el RGPD y el RIA	49
	M ^a CRISTINA BERENGUER ALBALADEJO	
1.	LA DISCRIMINACIÓN ALGORÍTMICA COMO UNO DE LOS PRINCIPALES RIESGOS DERIVADOS DEL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA TOMA DE DECISIONES	50
2.	LA OPACIDAD COMO PRINCIPAL ESCOLLO PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA.....	55
2.1.	Consideraciones previas	55
2.2.	Opacidad en el uso y sobre el contenido de los algoritmos	57
2.3.	Opacidad jurídica y técnica del algoritmo.....	59
3.	TRANSPARENCIA ALGORÍTMICA Y EXPLICABILIDAD: ¿QUÉ IMPLICAN ESTAS EXIGENCIAS?	68
4.	MEDIDAS PARA GARANTIZAR LA TRANSPARENCIA Y LA EXPLICABILIDAD EN LA TOMA DE DECISIONES ALGORÍTMICAS.....	75
4.1	Estado de la cuestión	75
4.2	La transparencia y la explicabilidad en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de protección de datos (RGPD): especial referencia a las decisiones automatizadas del art. 22	78
4.3.	La transparencia y la explicabilidad en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial	101

5.	CONSIDERACIONES FINALES SOBRE LA NECESIDAD DE TRANSPARENCIA Y EXPLICABILIDAD PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA	112
	BIBLIOGRAFÍA	113
 Aplicaciones de la inteligencia artificial conforme a la Ley de Movilidad Sostenible. Consideraciones en torno al régimen de responsabilidad civil acorde con la innovación		 119
YOLANDA BUSTOS MORENO		
1.	EL REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 13 DE JUNIO DE 2024 POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL Y EL PROYECTO DE LEY DE MOVILIDAD SOSTENIBLE DE 23 DE FEBRERO DE 2024	120
1.1.	Consideraciones generales de la AIA	120
1.2.	La regulación y su papel de apoyo a la innovación en el desarrollo de sistemas de IA	122
1.3.	El Proyecto de Ley de Movilidad Sostenible de 23 de febrero de 2024 con relación a la aplicación de la IA en vehículos automatizados.....	124
1.4.	El concepto de “sistema de inteligencia artificial” en la AIA y PLMS	126
2.	DILEMAS EN TORNO A LA REGULACIÓN DE LA RESPONSABILIDAD CIVIL EN LAS ACTIVIDADES QUE EMPLEAN SISTEMAS DE IA .	129
2.1.	Características especiales de los sistemas de IA con relación al riesgo	130
2.2.	El debate sobre el régimen de responsabilidad civil más favorable a la innovación en sistemas de IA.....	137
2.3.	El replanteamiento de la responsabilidad objetiva en el <i>Complementary Impact Assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence</i>	139
3.	EL APOYO A LOS SISTEMAS DE IA INNOVADORES ANTES DE LA INTRODUCCIÓN EN EL MERCADO O PUESTA EN SERVICIO DESDE EL PERFIL DE LA RESPONSABILIDAD CIVIL	141
	BIBLIOGRAFÍA	145

**Responsabilidad civil e inteligencia artificial en el ámbito sanitario:
posibles vías de reclamación 149**

RAQUEL EVANGELIO LLORCA

1	APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR SANITARIO.....	150
2.	RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR EL USO DE SISTEMAS DE INTELIGENCIA DE ARTIFICIAL EN EL ÁMBITO DE LA SANIDAD: CUESTIONES GENERALES	155
3.	DAÑOS CAUSADOS POR LA INTELIGENCIA ARTIFICIAL COMO PRODUCTO DEFECTUOSO.....	166
3.1.	Ámbito de aplicación del régimen de responsabilidad civil por daños causados por productos defectuosos. Los sistemas inteligentes como productos defectuosos	166
3.2.	Sujetos responsables.....	178
3.3.	Sujetos legitimados para ejercitar acciones por daños causados por productos defectuosos.....	186
3.4.	Fundamento de la responsabilidad y causas de exoneración	187
4.	RÉGIMEN DE RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR SERVICIOS SANITARIOS DEL ART. 148 TRLGDCU	190
4.1.	Ámbito de aplicación y fundamento de la responsabilidad	190
4.2.	Sujeto responsable	195
4.3.	Sujeto protegido	197
5.	RESPONSABILIDAD PATRIMONIAL DE LA ADMINISTRACIÓN SANITARIA	199
6.	RÉGIMEN DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL DEL CÓDIGO CIVIL.....	204
7.	CONSIDERACIONES FINALES SOBRE LA CONCURRENCIA DE RÉGIMENES APLICABLES	210
8.	BIBLIOGRAFÍA	214

Los *deepfakes* y la intromisión en los derechos de la personalidad (imagen, voz, honor y protección de datos) y sus mecanismos de reparación 223

BEATRIZ EXTREMERA FERNÁNDEZ

1.	INTRODUCCIÓN.....	223
2.	PRECISIONES CONCEPTUALES: QUÉ ES EL <i>DEEPFAKE</i> Y SU CLASIFICACIÓN DEL RIESGO.....	225
3.	PROBLEMÁTICA JURÍDICA DEL <i>DEEPFAKE</i>	230

3.1.	Los derechos al honor, a la propia imagen y a la voz en la LO 1/1982	230
3.2.	La imagen y voz como datos de carácter personal en el uso del <i>deepfake</i>	243
4.	EL PAPEL DE LA ADVERTENCIA EN EL USO DEL <i>DEEPFAKE</i>	246
5.	MECANISMOS DE PROTECCIÓN	248
5.1.	Tutela de los derechos de la personalidad protegidos en la LO 1/1982	249
5.2.	Tutela de los datos de carácter personal	250
5.3.	La responsabilidad de los prestadores de servicios de la sociedad digital.....	253
6.	CONCLUSIONES	255
7.	BIBLIOGRAFÍA	257

Responsabilidad civil derivada de la adquisición y utilización de <i>werables</i> y servicios digitales en materia de salud	261

PEDRO J. FEMENÍA LÓPEZ.

1.	PLANTEAMIENTO: DE LA <i>E-HEALTH</i> A LA AUTONOMÍA INDIVIDUAL EN LA GESTIÓN DE LA SALUD	261
2.	RESPONSABILIDAD DERIVADA DE LA COMPRA DEL BIEN O DE LA CONTRATACIÓN DEL CONTENIDO O SERVICIO.....	269
2.1.	Ámbito de aplicación	269
2.2.	Sujeto responsable	274
2.3.	Criterios de imputación.....	275
3.	LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE <i>WEREABLES</i> Y SERVICIOS DIGITALES EN MATERIA DE SALUD	281
3.1.	Ámbito de aplicación	283
3.2.	Sujetos responsables.....	293
3.3.	Criterios de imputación.....	300
	BIBLIOGRAFÍA	315

Interfaces cerebro-computador: protección de los neurodatos a través de los neuroderechos y de la responsabilidad civil del art. 82 del RGPD.....	319

MARÍA REMEDIOS GUILABERT VIDAL

1.	INTRODUCCIÓN.....	319
1.1.	El estado actual de la Neurotecnología: avances y desafíos	319

1.2.	Las interfaces cerebro-computador	325
2.	LA PROTECCIÓN DISPENSADA POR LOS NEURODERECHOS.....	329
2.1.	Los neuroderechos como nuevos derechos fundamentales: concepto y clases	329
2.2.	Soft law público y avances legislativos	331
3.	PROTECCIÓN DISPENSADA A LOS NEURODATOS POR EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO	336
3.1.	Concepto y naturaleza jurídica del neurodato	336
3.2.	Responsabilidad por daños causados por infracción del derecho a la protección de datos en el ámbito de las BCI	338
	BIBLIOGRAFÍA	349

	Encaje del sistema de Inteligencia Artificial utilizado con determinados fines médicos en algunas de las cuestiones suscitadas al amparo del régimen de responsabilidad por productos defectuosos.....	353

MARÍA JORQUI AZOFRA

1.	INTRODUCCIÓN	353
2.	EL SISTEMA DE IA COMO PRODUCTO.....	356
3.	EL SISTEMA DE IA COMO PRODUCTO SANITARIO	360
4.	¿QUÉ DETERMINA EL CARÁCTER DEFECTUOSO DEL SISTEMA DE IA?	365
5.	SISTEMA DE EXHIBICIÓN DE PRUEBAS Y CARGA DE LA PRUEBA....	380
6.	CAUSAS DE EXONERACIÓN: ESPECIAL CONSIDERACIÓN A LOS RIESGOS DEL DESARROLLO	385
7.	CONCLUSIONES	390
	BIBLIOGRAFÍA	393
	NORMATIVA Y OTROS DOCUMENTOS.....	396
	JURISPRUDENCIA.....	396

	IA y vehículos autónomos: cuestiones concernientes a la responsabilidad no contractual en la vertiente del derecho internacional privado.....	399

RAÚL LAFUENTE SÁNCHEZ

1.	INTRODUCCIÓN	400
2.	VEHÍCULOS AUTÓNOMOS Y RESPONSABILIDAD CIVIL EXTRA-CONTRACTUAL	403

2.1	Incidencia del Reglamento de Inteligencia Artificial	403
2.2	Propuesta de revisión de la Directiva 85/374 sobre productos defectuosos	407
3.	SOLUCIÓN DE CONTROVERSIAS Y APLICACIÓN DE LAS NORMAS DE DERECHO INTERNACIONAL PRIVADO	415
3.1	Competencia judicial internacional	415
3.2	Ley aplicable	423
4.	REFLEXIONES FINALES: IDONEIDAD DE LOS INSTRUMENTOS DE DIPR ACTUALMENTE EN VIGOR PARA REGULAR LAS RECLAMACIONES DERIVADAS DE LA CONDUCCIÓN AUTOMATIZADA	444
4.1	Para determinar la jurisdicción de los tribunales de la UE	444
4.2	En materia de ley aplicable	445
	BIBLIOGRAFÍA.....	446
	Vehículos autónomos y responsabilidad civil. La vacilante ruta marcada por el legislador europeo	451
	PEDRO JOSÉ LÓPEZ MAS	
1.	CONSIDERACIONES PRELIMINARES SOBRE LA CONDUCCIÓN AUTOMATIZADA	452
1.1.	Conceptualización y situación actual	452
1.2.	Retos jurídicos que presenta este «novedoso» fenómeno	456
2.	RÉGIMEN JURÍDICO DE LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE VEHÍCULOS A MOTOR, Y BREVES NOTAS SOBRE SU ASEGURAMIENTO	459
2.1.	Planteamiento de la cuestión	459
2.2.	El concepto de «vehículo a motor»	463
2.3.	El concepto de «hecho de la circulación»	467
2.4.	El concepto de «conductor»	469
3.	LA INCIDENCIA EN LA CONDUCCIÓN AUTOMATIZADA DE LA NUEVA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL, Y SUS EVIDENTES DISFUNCIONALIDADES	470
3.1.	Ámbito de aplicación y caracteres	473
3.2.	Deber de exhibición de pruebas y presunción <i>iuris tantum</i> en caso de incumplimiento	475
3.3.	Presunción <i>iuris tantum</i> de la relación de causalidad en caso de culpa	476
4.	BIBLIOGRAFÍA	479

Inteligencia artificial en la prestación de servicios de salud: funcionalidades, riesgos y responsabilidad civil.....	481
RAQUEL LUQUIN BERGARECHE	
1. INTRODUCCION. ROBOTS Y APLICACIONES DE INTELIGENCIA ARTIFICIAL COMO INSTRUMENTOS AUXILIARES EN LA PRESTACION DE SERVICIOS MEDICOS	482
2. LA PREVENCIÓN DE LOS RIESGOS DE LA INTELIGENCIA ARTIFICIAL EN SALUD A LA LUZ DEL REGLAMENTO (UE) 2024/1689 DE 13 DE JUNIO DE 2024, POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE IA (RIA)	491
2.1. Primer marco regulatorio europeo de la IA	491
2.2. Riesgos y salud: la ambigua definición de los sistemas IA de alto riesgo	493
2.3. Obligaciones de proveedores y responsables del despliegue: información y supervisión.....	500
2.4. Aplicaciones de IA en salud para uso particular o doméstico	506
2.5. El RIA como sistema normativo de prevención del riesgo: remisión a otros marcos regulatorios en el ámbito de los daños causados por sistemas de IA en salud	509
2.6. Formación y capacitación en IA del profesional de la salud	512
3. DAÑOS CAUSADOS EN INTERVENCIONES MEDICAS CON AUXILIO DE IA: REDEFINICION DE LA “LEX ARTIS” Y FUNDAMENTOS DE LA RESPONSABILIDAD	513
3.1. Cuando el médico se prevale de un sistema de IA y su actuación causa daños: presupuestos de la obligación de responder	513
3.2. Caracteres de los sistemas de IA en salud: en particular, la influencia del grado de autonomía del robot o sistema auxiliar de IA en la responsabilidad por daños	518
3.3. Relación de causalidad. La causalidad física y su prueba.....	521
3.4. La causalidad jurídica: el juicio de imputación.....	523
3.5. Agentes implicados en la prestación de servicios médicos con auxilio de IA.....	524
3.6. Causas de exclusión o exoneración	529
4. ALGUNAS REFLEXIONES SOBRE EL RÉGIMEN (NO ARMONIZADO Y “DE MÍNIMOS”) DE LA PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRA-CONTRACTUAL A LA IA (PDRCIA)	531
5. REFERENCIAS BIBLIOGRAFICAS	533

La doctrina *crashworthiness*: origen, desarrollo y posible aplicación a los vehículos automatizados..... 539

ANDRÉS MARÍN SALMERÓN

1.	LA DOCTRINA <i>CRASHWORTHINESS</i> O <i>SECOND COLLISION</i>	540
1.1.	Breve referencia a su concepto y objetivo del trabajo	540
1.2.	Principios y orígenes de la doctrina <i>crashworthiness</i>	544
1.3.	Aplicación de la doctrina <i>Crashworthiness</i> . Relación de la primera colisión con la <i>second collision</i> : intervención de tercero y culpa del perjudicado	555
2.	SU CONEXIÓN CON EL CRITERIO DE RIESGO UTILIDAD Y EL DISEÑO ALTERNATIVO RAZONABLE: DE NUEVO CON LA RESPONSABILIDAD SUBJETIVA	567
3.	LA DOCTRINA <i>CRASHWORTHINESS</i> EN LA JURISPRUDENCIA ESPAÑOLA.....	569
4.	LA APLICACIÓN DE LA DOCTRINA EN ESPAÑA: SU COMPATIBILIDAD CON EL REAL DECRETO LEGISLATIVO 8/2004, DE 29 DE OCTUBRE, POR EL QUE SE APRUEBA EL TEXTO REFUNDIDO DE LA LEY SOBRE RESPONSABILIDAD CIVIL Y SEGURO EN LA CIRCULACIÓN DE VEHÍCULOS A MOTOR.....	573
5.	LA APLICACIÓN DE LA DOCTRINA <i>CRASHWORTHINESS</i> CON LA NUEVA NORMATIVA DE RESPONSABILIDAD POR DAÑOS POR PRODUCTOS DEFECTUOSOS	577
6.	BIBLIOGRAFÍA	579

El uso de algoritmos en detrimento de los principios jurídicos y económicos de la Unión Europea 583

LUZ M. MARTÍNEZ VELENCOSO

1.	INTRODUCCIÓN.....	583
2.	TRANSPARENCIA ALGORÍTMICA.....	585
2.1.	Derecho de la competencia	585
2.2.	Transparencia en la publicidad algorítmica	593
3.	DERECHO DE CONSUMO E INTELIGENCIA ARTIFICIAL	596
3.1.	Microtargeting.....	596
3.2.	Contratos algorítmicos	599
4.	BIBLIOGRAFÍA	600

Uso de inteligencia artificial, <i>Big Data</i> y otras tecnologías disruptivas en las plataformas digitales de alojamiento turístico: desafíos actuales en materia de privacidad, transparencia algorítmica y responsabilidad civil.....	603
LUCÍA MOLINA MARTÍNEZ	
1. <i>BIG DATA</i> , INTELIGENCIA ARTIFICIAL, IoT Y TECNOLOGÍA <i>BLOCKCHAIN</i> EN LAS PLATAFORMAS DIGITALES DE ALOJAMIENTO TURÍSTICO	604
1.1. La transformación digital del sector turístico: el papel de las plataformas digitales de alojamiento turístico	604
1.2. La aplicación de tecnologías innovadoras disruptivas por las plataformas de alojamiento turístico: desde el algoritmo hasta la tecnología <i>blockchain</i>	607
2. IMPACTO DE LAS TECNOLOGÍAS DISRUPTIVAS EN LA PRIVACIDAD Y PROTECCIÓN DE DATOS DE LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO	613
2.1. Empleo de tecnologías disruptivas en la recopilación y tratamiento masivo de datos personales: aparición de nuevas categorías de datos y riesgos para la privacidad de los usuarios	613
2.2. La elaboración de perfiles y la adopción de decisiones automatizadas a través de sistemas avanzados de IA.....	620
3. TRANSPARENCIA ALGORÍTMICA Y RESPONSABILIDAD CIVIL EN EL MARCO DE LA INTERMEDIACIÓN DE LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO.....	628
3.1. Desafíos que plantea la toma de decisiones algorítmicas y la regulación europea en materia de IA para combatirlos.....	628
3.2. Exigencias de transparencia para los sistemas algorítmicos de recomendación, clasificación, selección de contenidos y publicidad en línea de los prestadores de servicios de alojamiento de datos	632
3.3. Tratamiento legal de la responsabilidad de las plataformas por la moderación automatizada de contenidos y el incumplimiento de las obligaciones de transparencia algorítmica: régimen transitorio a la espera de una regulación específica acerca de la discriminación algorítmica	640
BIBLIOGRAFÍA	645

Implicaciones jurídicas del uso de los robots y la inteligencia artificial en el ámbito sanitario. ¿Hacia una nueva medicina?	651

ÓSCAR MONJE BALMADEA

1. LA PROTECCIÓN DE LA SALUD Y LA EVOLUCIÓN TECNOLÓGICA: ESPECIAL REFERENCIA A LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL	651
1.1. Consideraciones previas: la robótica y la inteligencia artificial en el ámbito sanitario	651
1.2. La utilización de la inteligencia artificial en el ámbito de la salud: sus limitaciones y los desafíos éticos y jurídicos que presenta.	654
2. PLANTEAMIENTO LEGISLATIVO EN MATERIA DE INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD CIVIL EN LA UNIÓN EUROPEA.....	660
2.1. La responsabilidad civil en el ámbito sanitario. Responsabilidad objetiva y gestión de riesgos.....	660
2.2. El posicionamiento inicial de la Unión Europea en materia de responsabilidad civil de los robots y los sistemas de inteligencia artificial	664
2.3. Las propuestas de regulación de la UE: La Directiva sobre responsabilidad por daños causados por productos defectuosos y la Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial	672
BIBLIOGRAFÍA UTILIZADA.....	679

La responsabilidad civil derivada de los accidentes de circulación ocasionados con vehículos autónomos	681

ESTHER MONTERROSO CASADO

1. INTRODUCCIÓN.....	682
2. EVOLUCIÓN Y REGULACIÓN DE LA RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL POR DAÑOS EN LA CIRCULACIÓN DE VEHÍCULOS A MOTOR.....	683
2.1. Evolución legal de la responsabilidad derivada de los accidentes de circulación	683
2.2. Regulación actual y perspectivas de futuro de la responsabilidad derivada de los accidentes de circulación	687
3. VEHÍCULOS AUTÓNOMOS Y CONDUCCIÓN AUTOMATIZADA.....	692
3.1. El vehículo autónomo	692
3.2. Los niveles de autonomía	694
3.3. Autonomía real en la oferta de conducción automatizada	696

4.	REGULACIÓN DE LA CONDUCCIÓN AUTOMATIZADA	698
4.1.	Marco jurídico europeo de vehículos automatizados y totalmente automatizados	698
4.2.	Marco jurídico nacional de conducción automatizada	703
5.	REGULACIÓN DE LOS SISTEMAS DE ALTO RIESGO EN LA INTELIGENCIA ARTIFICIAL	712
5.1.	Reglamento europeo por el que se establecen normas armonizadas en materia de inteligencia artificial	712
5.2.	Directiva sobre responsabilidad por los daños causados por productos defectuosos	717
5.3.	Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial	720
6.	HACIA UN NUEVO CRITERIO DE RESARCIMIENTO DE DAÑOS DERIVADO DE LA AUSENCIA DEL CONDUCTOR DEL VEHÍCULO ...	726
6.1.	Responsabilidad del fabricante del vehículo	729
6.2.	Responsabilidad del operador o del propietario del vehículo	732
6.3.	Resarcimiento del daño por la aseguradora del vehículo, tomando como referencia la LRCSCVM	734
6.4.	Resarcimiento del daño por la aseguradora del vehículo, sin imputación de la responsabilidad	737
7.	CONCLUSIONES	739
8.	BIBLIOGRAFÍA	743

Impresión 3D en el ámbito médico: problemática de la responsabilidad civil y patrimonial y sus incidencias digitales y de inteligencia artificial por las reformas de la Unión Europea	749

JUAN ANTONIO MORENO MARTÍNEZ

1.	LA FABRICACIÓN ADITIVA O IMPRESIÓN EN 3D: LAS INICIATIVAS DE LA UNIÓN EUROPEA	750
2.	LA BIOIMPRESIÓN 3D COMO ESPECÍFICA IMPRESIÓN EN LA MEDICINA. LA RESPONSABILIDAD CIVIL -Y PATRIMONIAL-: RÉGIMEN LEGAL APLICABLE	755
2.1.	Consideraciones generales	755
2.2.	Incidencia de la consideración de la bioimpresión como producto sanitario: Evaluación de la conformidad. La responsabilidad patrimonial de la Agencia Española del medicamento y productos sanitarios (AEMPS) y su delimitación con respecto a los casos de responsabilidad patrimonial de la Administración sanitaria	760

2.3. Responsabilidad civil en la bioimpresión	767
BIBLIOGRAFÍA	782

Taxonomía de los modelos de IA de uso general. Probabilidad de generar riesgos de alto impacto y la necesidad de identificarlos.....	787

CARMEN MUÑOZ GARCÍA

1. JUSTIFICACIÓN DEL ESTUDIO	787
1.1. La IA Generativa como modelo de IA de uso general. El caso	787
1.2. ¿Por qué regularlo?	790
1.3. La incidencia en los derechos de la persona	793
2. TAXONOMÍA DE LOS MODELOS DE IA DE USO GENERAL	794
2.1. Definiciones legales y clasificación.....	794
2.2. La exigencia general de transparencia y una regulación singular para los modelos de GPAI.....	796
2.3. Marco regulatorio propio	798
3. EL RIESGO EN LOS MODELOS Y SISTEMAS GPAI ¿CRITERIO SUFICIENTE PARA FIJAR LA OBJETIVACIÓN DE LA RC?	807
3.1. Definiciones sobre el riesgo. Identificar incidente y peligro de IA	810
3.2. ¿A qué sujetos se dirigen las obligaciones de evitar el riesgo? ¿A qué herramientas?.....	811
4. REFLEXIONES FINALES.....	814
5. BIBLIOGRAFÍA	816

Responsabilidad por conductas discriminatorias derivadas de los sesgos en el uso de la inteligencia artificial: jurisprudencia y reglamento europeo	817

ALBERTO MUÑOZ VILLARREAL

1. INTRODUCCIÓN	817
2. ANÁLISIS JURISPRUDENCIAL	818
3. EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL	829
BIBLIOGRAFÍA	834

Inteligencia artificial y responsabilidad civil: un enfoque ético en la era digital.....	837
IÑIGO A. NAVARRO MENDIZÁBAL	
1. INTRODUCCIÓN.....	837
2. PRINCIPIOS ÉTICOS DE LA IA	840
2.1. La importancia de la Ética en la IA	840
2.2. Principales principios éticos	847
3. INTENTO DE APORTAR SOLUCIONES A LOS DESAFÍOS A LOS QUE SE ENFRENTA LA RC POR DAÑOS CAUSADOS POR LA IA.....	859
3.1. RC objetiva o subjetiva	859
3.2. La Explicabilidad y Opacidad de los Sistemas de IA (Black Box) ..	862
3.3. Difusión de la Responsabilidad	866
3.4. Autonomía de la IA y Responsabilidad Humana.....	869
3.5. Daños colectivos y difusos.....	871
3.6. Daños futuros e inciertos	873
4. BIBLIOGRAFÍA UTILIZADA.....	874
Los sistemas de inteligencia artificial, ¿productos defectuosos?	879
MANUEL ORTIZ FERNÁNDEZ	
1. CUESTIONES PRELIMINARES	879
2. LA LEY DE INTELIGENCIA ARTIFICIAL	885
2.1. Concepto y características básicas de la inteligencia artificial	885
2.2. El riesgo y la intervención humana: las actividades prohibidas y la clasificación de los sistemas	893
3. LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE SISTEMAS INTELIGENTES	898
3.1. Las relaciones entre las dos propuestas de Directiva.....	898
3.2. La responsabilidad civil en la (revisada) propuesta de Directiva sobre productos defectuosos	903
3.3. La propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial y las presunciones	914
BIBLIOGRAFÍA	918

Perspectiva y categorización del riesgo en el Reglamento de Inteligencia Artificial 923

MIQUEL PEGUERA

1.	INTRODUCCIÓN.....	923
2.	LA PERSPECTIVA DEL RIESGO	926
3.	LA PROHIBICIÓN DE PRÁCTICAS DE IA QUE IMPLICAN UN RIESGO EXCESIVO	930
4.	SISTEMAS DE IA DE ALTO RIESGO VINCULADOS A LA LEGISLACIÓN ARMONIZADA SOBRE SEGURIDAD DE PRODUCTOS.....	935
5.	SISTEMAS DE IA DE ALTO RIESGO INDEPENDIENTES	937
	5.1. Ejemplos de casos de uso relevantes	939
	5.2. Criterios para rechazar la calificación de riesgo alto	941
	5.3. Modificaciones de la relación de casos del Anexo III.....	944
6.	OBLIGACIONES DE TRANSPARENCIA FRENTE A RIESGOS DE CONFUSIÓN	944
7.	RIESGOS SISTÉMICOS DE LOS MODELOS DE USO GENERAL.....	946

Inteligencia artificial generativa y daños por infracciones normativas del derecho de protección de datos personales. Un análisis a partir de la jurisprudencia reciente del TJUE sobre el artículo 82 RGPD..... 949

ANTONI RUBÍ PUIG

1.	INTRODUCCIÓN.....	950
2.	FUNCIONAMIENTO DE LA IA GENERATIVA E IMPLICACIONES PARA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES.....	954
	2.1. Concepto	954
	2.2. Tipología	955
	2.3. Cadena de valor	956
3.	CUESTIONES Y PROBLEMAS SOBRE LA REPARACIÓN DE DE DAÑOS	968
	3.1. Introducción: el artículo 82 RGPD como fundamento de responsabilidad civil	968
	3.2. Daños mínimos y de bagatela	970
	3.3. Indemnizabilidad del temor.....	972
	3.4. Brechas de seguridad.....	977
	3.5. Relaciones con otros fundamentos de responsabilidad: el caso de los <i>deepfakes</i>	980
	3.6. Pluralidad de sujetos responsables.....	983

4.	CONCLUSIONES	985
	BIBLIOGRAFÍA UTILIZADA.....	986
	JURISPRUDENCIA DEL TJUE	990
	El seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial	993
	ALBERTO J. TAPIA HERMIDA	
1.	INTRODUCCIÓN.....	994
2.	ANTECEDENTES	995
	2.1. La Resolución del Parlamento Europeo sobre un régimen de responsabilidad civil en materia de inteligencia artificial de 20 de octubre de 2020	995
	2.2. La Propuesta de Directiva sobre responsabilidad en materia de inteligencia artificial de 28 de septiembre de 2022	997
3.	EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL.....	998
4.	LAS CARACTERÍSTICAS DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL	999
	4.1. Seguro voluntario	999
	4.2. Seguro de responsabilidad civil empresarial o profesional.....	1000
5.	LAS PARTES	1000
	5.1. El asegurador	1000
	5.2. El tomador y el asegurado. Las pólizas colectivas.....	1001
6.	EL RÉGIMEN DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL	1001
	6.1. Seguro de régimen común o seguro por grandes riesgos.....	1001
	6.2. Aplicación de la LCS.....	1002
	6.3. Aplicación de la LOSSEAR.....	1002
7.	LA DELIMITACIÓN SUSTANCIAL DEL RIESGO CUBIERTO POR REFERENCIA A LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL	1003
	7.1. Definición general del riesgo cubierto	1003
	7.2. Descripción específica de los riesgos excluidos de la cobertura ...	1003
8.	LA DELIMITACIÓN TEMPORAL DEL RIESGO CUBIERTO POR REFERENCIA A LAS RECLAMACIONES PRESENTADAS CONTRA EL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO. LAS CLÁUSULAS “CLAIMS MADE”	1004

9.	LA DEFENSA JURÍDICA DEL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO FRENTE A LA RECLAMACIÓN DEL USUARIO PERJUDICADO O DE SUS HEREDEROS	1006
10.	LA ACCIÓN DIRECTA DEL USUARIO DE UN SISTEMA DE INTELIGENCIA ARTIFICIAL PERJUDICADO O SUS HEREDEROS CONTRA EL ASEGURADOR DEL OPERADOR	1007
11.	LA TRANSPARENCIA DE LAS CONDICIONES DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL.....	1008
12.	CONCLUSIONES.....	1008

La discriminación algorítmica en el sector sanitario

ITZIAR ALKORTA IDIAKEZ

Profesora Titular de Derecho Civil UPV/EHU

Sumario: 1. INTRODUCCION; 2. CASOS DE DISCRIMINACIÓN ALGORÍTMICA EN EL SECTOR SANITARIO; 3. APLICABILIDAD DE LA NORMATIVA ANTIDISCRIMINATORIA EN MATERIA DE DISCRIMINACIÓN ALGORÍTMICA; 3.1. Normativa antidiscriminatoria europea; 3.2. Limitaciones de la eficacia horizontal; 3.3. La prueba del daño moral; 3.4. Litigación colectiva; 4. APLICABILIDAD DE LA NORMATIVA SECTORIAL DE LA IA; 4.1. Principios y requisitos aplicables a la seguridad de los productos sanitarios con IA; 4.2. La falta de transparencia en las decisiones automatizadas; 4.3. El problema de la calidad de los conjuntos de datos; 4.4. La responsabilidad por daños morales causados por la IA; a) Propuesta de Directiva de Responsabilidad por Productos Defectuosos; b) Propuesta de Directiva sobre Responsabilidad Civil por Daños Causados por la IA; 5. Conclusiones.

1. INTRODUCCIÓN

La transformación digital del sector sanitario, impulsada por el desarrollo de sistemas basados en inteligencia artificial (SIA), ha revolucionado la atención médica al ofrecer diagnósticos más rápidos, tratamientos personalizados y una optimización sin precedentes de los recursos disponibles. Sin embargo, esta revolución tecnológica trae consigo riesgos de reproducir -e incluso amplificar por “codificación redundante”- las desigualdades estructurales ya existentes, exponiendo a los pacientes a una nueva forma de discriminación: la discriminación algorítmica.

Lejos de ser un problema hipotético, la discriminación algorítmica en sanidad es una realidad preocupante. Estudios recientes han demostrado cómo ciertos algoritmos, aparentemente neutrales, generan sesgos que afectan de manera desproporcionada a grupos vulnerables, como minorías étnicas, mujeres y personas con discapacidad.¹ Este fenómeno tiene su origen en datos históricos sesgados, conjuntos de datos no representativos y diseños de modelos que ignoran las diferencias sociodemográficas y contextuales de las poblaciones a las que pretenden servir. En el sector sanitario, este tipo de discriminación puede surgir de múltiples fuentes, principalmente relacionadas con la naturaleza de los datos utilizados y las decisiones de diseño algorítmico.

El problema de la discriminación algorítmica se ve agravado por la opacidad inherente a muchos de estos sistemas, que operan como “cajas negras”, cuyas decisiones no siempre pueden ser explicadas ni comprendidas. La falta de transparencia de los sistemas de IA dificulta la detección de sesgos y limita la capacidad de las víctimas para defender sus derechos. Así, surge la necesidad imperiosa de establecer un marco regulatorio robusto que aborde estas deficiencias y asegure que el uso de la IA en sanidad se ajuste a los principios de igualdad y no discriminación.

El presente trabajo analiza cómo la normativa de la Unión Europea -desde la normativa antidiscriminatoria, pasando por el Reglamento General de Protección de Datos, hasta la reciente Ley de Inteligencia Artificial- aborda, aunque de manera aún incipiente, el problema de la discriminación algorítmica, prestando especial atención a las posibles respuestas legales para corregir y prevenir estos sesgos, así como las reglas especiales sobre responsabilidad civil derivada de los daños morales que puedan ocasionar los productos sanitarios que integran estos sistemas.

Este análisis culmina con una serie de propuestas *de lege ferenda* orientadas a fortalecer la regulación específica en este ámbito, subrayando la necesidad de integrar la equidad en el diseño, implementación y supervisión de los productos sanitarios y la mejora de los remedios que ofrece el ordenamiento actual frente a los daños morales causados por la SIA.

¹ Véanse, entre otros, ADAMSON, A. S., Y SMITH, A. “Machine learning and health care disparities in dermatology”. *JAMA Dermatology*, 2018, 154(11), 1247-1248. BAROCAS, S. Y SELBST, A. D. “Big Data’s Disparate Impact.” *California Law Review*, 2016, 104(3), 671-732. SIRUGO, G., WILLIAMS, S. M., y TISHKOFF, S. A. “The Missing Diversity in Human Genetic Studies”. *Cell*, 2019177(1), 26-31. HOLDCROFT, A. “Gender bias in research: How does it affect evidence based medicine?” *Journal of the Royal Society of Medicine*, 2007, 100(1), 2-3. CHIN, MH, *et al.* “Guiding Principles to Address the Impact of Algorithm Bias on Racial and Ethnic Disparities in Health and Health Care.” *JAMA Netw Open*. 2023 Dec 1;6(12): e2345050.

2. CASOS DE DISCRIMINACIÓN ALGORÍTMICA EN EL SECTOR SANITARIO

El uso de la inteligencia artificial en el ámbito sanitario, pese a sus potenciales beneficios en términos de eficiencia y precisión, no está exento de riesgos, especialmente en lo relativo a la discriminación algorítmica.² Aunque el propósito declarado de los desarrolladores de estos sistemas es mejorar la atención médica, su implementación puede reproducir las desigualdades que las políticas antidiscriminatorias pretenden erradicar, con consecuencias adversas para la salud y el bienestar de los pacientes. Un sistema de IA que evalúe incorrectamente la gravedad de los síntomas de un paciente debido a sesgos en los datos de entrenamiento puede generar diagnósticos erróneos. Además, estos sesgos pueden acentuar las disparidades en la calidad de la atención recibida por colectivos vulnerables. A nivel sistémico, la falta de transparencia en las decisiones algorítmicas puede socavar la confianza pública en las instituciones sanitarias y dificultar la labor de los reguladores para abordar problemas de seguridad y equidad en la atención médica.³

Un ejemplo de **sesgo racial** se encuentra en los sistemas de IA utilizados para la detección de enfermedades dermatológicas, donde los pacientes con piel más oscura reciben diagnósticos menos precisos debido a que los algoritmos se entrenaron mayoritariamente con imágenes de piel clara.⁴ Asimismo, un estudio de OBERMEYER *et al.* muestra cómo los afroamericanos en Estados Unidos que presentan la misma gravedad de enfermedad que los pacientes blancos, son menos propensos a ser recomendados para programas de gestión de cuidados especiales. Esto se debe a que el algoritmo que asignaba los recursos empleaba el coste de los tratamientos anteriores como indicador de riesgo.⁵ Dado que en Estados Unidos se invierte menos en la atención de los afroamericanos, el sistema infería erróneamente que sus riesgos asisten-

² SCHNEIDER, I. "Diskriminierungsgefahren und Regulationsansätze bei der medizinischen Nutzung von KI", *Zeitschrift für medizinische Ethik* (2021), 67, 327.

³ WILDNER, M. "Diagnose, Prognose, Prädiktion", *Gesundheitswesen* 76 (2014), 4, 185-186; HORLEY, L. FLORIDI, L. "An Ethically" Mindful Approach to AI for Health Care", 2020, online: www.srn.com/abstract=3830536.

⁴ GLAUSER, W. "AI in health care: Improving outcomes or threatening equity?", *CMAJ* 2020, 192, 1, E21-E22; ADAMSON, A.S., SMITH, A., "Machine Learning and Health Care Disparities in Dermatology", *JAMA Dermatology*, 2018, 154 1247. GOODE, L. "Facial recognition software is biased towards white men", online: www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-with-white-men-black-women-error.

⁵ OBERMEYER *et al.* evidencian que: "el algoritmo, utilizado en la atención de más de 200 millones de personas, subestimó las necesidades de los pacientes negros en un 50%, perpetuando las disparidades raciales en la atención médica". OBERMEYER, Z. *et al.*, "Dissecting racial bias in an algorithm used to manage the health of populations", *Science* (2019), 366, 6464, 447-453.

ciales eran menores. Una IA sin sesgos debería haber identificado el doble de afroamericanos con necesidades de cuidados especiales.

Los **sesgos de género** en los algoritmos médicos también están ampliamente documentados, especialmente en áreas como la cardiología.⁶ La falta de representatividad de las mujeres en los datos de entrenamiento de los algoritmos ha llevado a diagnósticos incorrectos y tratamientos menos efectivos para ellas, exacerbando las disparidades de género en la atención sanitaria.⁷ Los algoritmos predictivos de riesgo de enfermedades cardíacas tienden a ser menos precisos para las mujeres, ya que los datos reflejan predominantemente síntomas típicos de los hombres. Esta falta de diversidad en los datos no solo traslada las desigualdades de género del mundo analógico al digital, sino que también perpetúa discriminaciones históricas. Es un hecho que los datos médicos existentes suelen estar dominados por hombres adultos blancos, en detrimento de datos sobre mujeres, niños y personas de diversos grupos étnicos⁸.

Los **sesgos socioeconómicos** en los algoritmos de IA se manifiestan a menudo a través de variables como nivel de ingresos, historial laboral o código postal, lo que puede llevar a la discriminación de personas con bajos ingresos o residentes en áreas desfavorecidas. En Estados Unidos, los algoritmos de predicción de reingreso hospitalario tienden a priorizar a los pacientes con mayores recursos debido a su capacidad para costear tratamientos, excluyendo a aquellos con menor poder adquisitivo de programas de prevención y bienestar.⁹ Además, el uso de IA en sistemas sanitarios basados en criterios de riesgo económico puede excluir a personas de bajos ingresos de programas de prevención y bienestar, perpetuando barreras de acceso a estos servicios.¹⁰

⁶ CIRILLO, D, CATUARA-SOLARZ, S, MOREY, C, GUNEX, E, SUBIRATS, L, MELLINO, S. "Sex and gender differences and biases in artificial intelligence for biomedicine and healthcare". *NPJ Digit Med*, 2020, 3(81):1-10.

⁷ HOLDCROFT señala que: "los algoritmos utilizados para predecir el riesgo de enfermedades cardíacas tienden a ser menos precisos en las mujeres, lo que aumenta el riesgo de infradiagnóstico y falta de tratamiento adecuado". También menciona que: "la subrepresentación de mujeres en ensayos clínicos contribuye a una menor precisión en las recomendaciones algorítmicas de tratamiento para mujeres, particularmente en enfermedades cardiovasculares". HOLDCROFT, A. "Gender bias in research: how does it affect evidence based medicine?" *Journal of the Royal Society of Medicine*. 2007; 100(1):2-3.

⁸ BLASIMME A., VAYENA, E. "The Ethics of AI in Biomedical Research, Patient Care and Public Health", M. Dubber, F. Pasquale, S. Das (Dir.), *The Oxford Handbook of Ethics of Artificial Intelligence*, Oxford/New York, 2020.

⁹ BAROCAS y SELBST destacan que variables como el código postal pueden actuar como *proxies* de la situación socioeconómica, afectando desproporcionadamente a poblaciones desfavorecidas y perpetuando las desigualdades estructurales. La utilización de estas variables en la toma de decisiones puede hacer que los algoritmos refuerzan desigualdades existentes, lo que se traduce en una menor asignación de recursos a quienes más lo necesitan. BAROCAS, S y SELBST, A.D. 'Big Data's Disparate Impact', *California Law Review*, 2016, 104, 671.

¹⁰ VEALE, M., BINNS, R. "Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data", *Big Data & Society* 2017, 4(2), 54.

Otro tipo de discriminación algorítmica consiste en la formación de “**grupos algorítmicos**” en función de correlaciones no causales identificadas por el sistema. Estos perfiles no se basan en características reales del paciente, sino en patrones que pueden dar lugar a estigmatización o discriminación. La medicina personalizada y la genética, que se apoyan en datos genómicos para adaptar tratamientos, también presentan riesgos si los algoritmos no contemplan la diversidad genética de la población. Los datos de entrenamiento dominados por muestras de personas de ascendencia europea limitan la eficacia de los sistemas para otras poblaciones étnicas, llevando a diagnósticos imprecisos y tratamientos inadecuados.

El **diagnóstico basado en la voz**, un área emergente en la detección de enfermedades como la demencia, la depresión y el Parkinson, plantea problemas similares. Los algoritmos entrenados para identificar biomarcadores vocales suelen plantear dificultades para reconocer variaciones dialectales o acentos locales, lo que conduce a diagnósticos incorrectos.¹¹ Un ejemplo preocupante es el análisis de balbuceos en bebés para predecir trastornos del espectro autista, donde, a pesar de la alta precisión en la predicción, se plantean serias objeciones éticas y legales por la posibilidad de marcar indebidamente a un bebé con un diagnóstico estigmatizante.¹²

Los **sistemas de triaje** y priorización de urgencias basados en IA también pueden introducir sesgos. Durante la pandemia de COVID-19, se presentó una demanda ante el Tribunal Constitucional Federal de Alemania por la posible discriminación contra personas con discapacidad en la asignación de camas de cuidados intensivos. El Tribunal dictaminó la necesidad de legislar sobre el triaje, ya que algoritmos como la *Clinical Frailty Score*, clasificaban a pacientes frágiles como menos prioritarios debido a su condición general, excluyéndolos de tratamientos que podrían salvarles la vida.¹³

La **medicina de precisión**, que clasifica a los pacientes según su predisposición genética, incrementa el riesgo de estigmatización para grupos vulnerables, como minorías étnicas o personas con condiciones genéticas poco co-

¹¹ *Winterlight Labs* desarrolló un modelo para detectar Alzheimer utilizando muestras de lenguaje de hablantes nativos de inglés canadiense, pero los errores de interpretación en hablantes no nativos indicaron deterioro cognitivo inexistente, ROBIN, J. “Using Digital Speech Assessments to Detect Early Signs of Cognitive Impairment”, *Front. Digit. Health, Sec. Connected Health*, Volume 3 - 2021.

¹² Además, la falta de regulación sobre la recopilación y uso de estos datos aumenta el riesgo de que terceros, como aseguradoras o empleadores, utilicen esta información para tomar decisiones que pueden ser discriminatorias.

¹³ Decisión del Tribunal Constitucional alemán (BVerfG) del 16 de diciembre de 2021 (1 BvR 154/20 = JZ 2022). Véase el comentario de la sentencia de HILGENDORF, E. “El triaje en el contexto de las decisiones de vida contra vida”, *InDret* 3.2022.

munes.¹⁴ Por ejemplo, si los algoritmos excluyen condiciones cromosómicas atípicas como el síndrome de Klinefelter (XXY en lugar de XY en varones), se puede comprometer la precisión de los diagnósticos y las recomendaciones de tratamiento. Este problema se agrava cuando los datos de entrenamiento no incluyen información suficiente sobre enfermedades genéticas raras, lo que lleva a predicciones y tratamientos inadecuados.¹⁵

Además, la utilización de IA para predecir el riesgo de enfermedades o reacciones a medicamentos se ha extendido a entornos no médicos, como la determinación de primas de seguros o la selección de candidatos laborales. La proliferación de estos sistemas, a menudo sin la regulación adecuada, plantea el riesgo de crear una “salud digital” en la que la información médica se utilice para excluir a ciertos grupos del acceso a servicios y beneficios.¹⁶

3. APLICABILIDAD DE LA NORMATIVA ANTIDISCRIMINATORIA EN MATERIA DE DISCRIMINACIÓN ALGORÍTMICA

La normativa antidiscriminatoria de la UE, anclada en el Tratado de Funcionamiento de la Unión Europea (TFUE) y en la Carta de Derechos Fundamentales, se ha desarrollado a través de diversas Directivas que abordan distintos motivos de discriminación, como el género, la raza y la orientación sexual. La aplicación de la normativa antidiscriminatoria en el ámbito sanitario es especialmente relevante, ya que, como hemos visto, los sistemas algorítmicos que apoyan las decisiones clínicas pueden contener sesgos que impacten de manera desproporcionada en ciertos grupos vulnerables o sometidos a factores de riesgo.

Este apartado revisa los principales hitos normativos y jurisprudenciales en torno a la discriminación algorítmica y explora las dificultades de acceso a

¹⁴ En este contexto, VEALE y BINNS señalan que esta individualización puede llevar a una menor solidaridad social y a una desprotección de aquellos pacientes que no cumplen con los perfiles genéticos predominantes. VEALE M., BINNS R. “Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data” *Big Data & Society* 2017, 4(2), 54.

¹⁵ SIRUGO *et al.* destacan que esta situación contribuye a una privación de la medicina personalizada para poblaciones infrarrepresentadas, agravando así las desigualdades en el acceso a tratamientos. La integración de algoritmos en el apoyo a la toma de decisiones clínicas puede mejorar la eficiencia del diagnóstico y tratamiento, pero cuando los conjuntos de datos utilizados están sesgados o son incompletos, los resultados pueden ser desastrosos. Por ejemplo, los algoritmos basados en datos genéticos tienden a sobre representar a personas de ascendencia europea, lo cual afecta negativamente la precisión de los diagnósticos para otras poblaciones étnicas. Véase SIRUGO *et al.*, “The Missing Diversity in Human Genetic Studies”, *Cell*, March 2019, Volume 177, Issue 1, 21 26-31 2019.

¹⁶ VEALE & BINNS, *Fairer machine learning...*, *op. cit.*, 56.

la justicia que enfrentan las víctimas de discriminación algorítmica en el ámbito sanitario.

3.1. NORMATIVA ANTIDISCRIMINATORIA

La prohibición de discriminación constituye un objetivo central de la Unión Europea, recogido en el artículo 3 del Tratado de la Unión Europea y en el artículo 8 del Tratado de Funcionamiento de la Unión Europea. Asimismo, el artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea establece una cláusula general que prohíbe toda forma de discriminación basada en motivos como el sexo, la raza, el origen étnico, la religión o las convicciones ideológicas.

A partir de estos textos fundamentales, se han promulgado diversas Directivas que desarrollan el principio de igualdad de trato en diferentes ámbitos. La Directiva 2000/43/CE, del Consejo, de 29 de junio de 2000, aborda la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico. Por su parte, la Directiva 2000/78/CE, del Consejo, de 27 de noviembre de 2000, establece un marco general para la igualdad de trato en el empleo y la ocupación, abarcando motivos de discriminación como la religión, las convicciones, la discapacidad, la edad o la orientación sexual. A estas se suma la Directiva 2004/113/CE, del Consejo, de 13 de diciembre de 2004, que extiende el principio de igualdad de trato entre hombres y mujeres al acceso a bienes y servicios y su suministro, siendo esta última norma especialmente relevante en el ámbito sanitario.

Adicionalmente, la Directiva 97/80/CE, que originalmente se refería a la discriminación por razón de sexo, introduce un principio general de prueba aplicable a todos los casos de discriminación. Esta Directiva establece que, cuando una persona presenta indicios razonables de discriminación, la carga de la prueba se invierte y corresponde al demandado demostrar que no ha habido vulneración del principio de igualdad. La Directiva 97/80/CE, aunque fue derogada y sustituida por la Directiva 2006/54/CE en el contexto de la igualdad de género en el empleo y la ocupación, sigue constituyendo un referente normativo en la inversión de la carga probatoria aplicable a otros tipos de discriminación, reflejando el compromiso de la Unión Europea con la protección efectiva contra la discriminación en todas sus manifestaciones.¹⁷

¹⁷ SERVICIO JURÍDICO DE LA COMISIÓN EUROPEA. *70 años de derecho de la Unión, una Unión al servicio de los ciudadanos*. Servicio Editorial de la Comisión Europea, 2023, págs. 160 a 162. BARRÈRE UNZUETA, M.A., MORONDO TARAMUNDI, D. “Subordiscriminación y discriminación interseccional: elementos para una teoría del derecho antidiscriminatorio”, *Anales de la Cátedra Francisco Suárez*, 45 (2011), 15-42.

En el apartado anterior se ha puesto de relieve que los servicios sanitarios que no tienen en cuenta las necesidades específicas de las mujeres y de determinadas minorías -que pueden padecer problemas diferentes o mostrar síntomas distintos en comparación con la población masculina blanca en la que se centra principalmente la investigación-, podrían discriminar en su disponibilidad o rendimiento.

Este tipo de discriminación podría entrar en el ámbito de aplicación de la Directiva 2004/113/CE, en lo que respecta al género, y de la Directiva 2000/43/CE, en lo que respecta al origen racial o étnico. De hecho, el considerando 17 de la Directiva 2004/113/CE establece que: “el principio de igualdad de trato en el acceso a bienes y servicios no exige que las instalaciones se proporcionen siempre a hombres y mujeres de forma compartida, siempre que no se proporcionen de forma más favorable a los miembros de un sexo”.

En nuestro entorno, debe hacerse referencia a la Ley 15/2022 integral para la igualdad de trato y la no discriminación, que regula los derechos y obligaciones de las personas físicas y jurídicas, y establece medidas para prevenir, eliminar y corregir cualquier forma de discriminación, ya sea directa o indirecta. Obsérvese que el ámbito de aplicación de la Ley española es más amplio que el de las Directivas referidas ya que alcanza a la discriminación por motivos de nacimiento, origen racial o étnico, sexo, religión, convicción u opinión, edad, discapacidad, orientación o identidad sexual, expresión de género, enfermedad o condición de salud, estado serológico y/o predisposición genética a sufrir patologías y trastornos, lengua, situación socioeconómica, o cualquier otra condición o circunstancia personal o social (art. 2.1). Además, la citada norma reconoce nuevos tipos de discriminación, como la discriminación por error, la discriminación múltiple y la discriminación interseccional, así como la inducción, la orden o la instrucción de discriminar.

A su vez, la Agencia Española de Supervisión de la Inteligencia Artificial, que ha sido la primera creada en Europa, recoge en sus estatutos la misión de: “supervisión, y en su caso sanción, de los sistemas de inteligencia artificial con el objeto de eliminar o reducir los riesgos para la integridad, la intimidad, la igualdad de trato y la no discriminación, en particular entre mujeres y hombres, y demás derechos fundamentales que pueden verse afectados por el mal uso de los sistemas”.¹⁸

¹⁸ Art. 4 del Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, BOE, n° 210, 2 de septiembre de 2023.

3.2. LIMITACIONES DE LA EFICACIA HORIZONTAL

Una cuestión relevante que plantea la aplicabilidad de las normas antidiscriminatorias europeas a los algoritmos utilizados en el ámbito sanitario es la limitada invocabilidad del Derecho de igualdad de la UE, dependiendo de si la parte demandada es una entidad pública o una persona privada. Se trata de un problema importante dada la naturaleza privada de los conflictos jurídicos que suelen surgir en el contexto de contratación de servicios algorítmicos de salud: ¿cabe o no invocar la obligación de no discriminar en la contratación de servicios sanitarios privados?

El TJUE ha reconocido que la prohibición de discriminación consagrada en el artículo 21 de la Carta tiene un efecto directo horizontal. Esta prohibición, según el dictamen del Tribunal, es suficiente por sí sola para conferir a los particulares un derecho invocable en un litigio que les enfrente en un ámbito regulado por el derecho de la Unión.¹⁹ Pero, como se ha visto anteriormente, los derechos de igualdad en el ámbito del género, la edad, la raza y otros motivos se reconocen en Directivas de la UE que en sí mismas carecen de efecto directo horizontal y sólo se aplicarán a las relaciones privadas tras su transposición a la legislación nacional.²⁰

En el caso español, la Ley 15/2022, de 12 de julio, ordena que las administraciones públicas y empresas promoverán la utilización de una IA “ética, confiable y respetuosa con los derechos fundamentales”. Específicamente, el art. 23 dispone que se favorecerá “la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente”. Estas previsiones son aplicables al ámbito de la sanidad tanto en la provisión de servicios médicos como en uso de tecnología sanitaria que emplee IA, incluidos los contratos privados relativos a productos y servicios sanitarios.

¹⁹ El artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea y la jurisprudencia derivada de los casos *Mangold*, *Kücükdeveci*, *Dansk Industri* y *Egenberger* han reconocido el efecto directo horizontal del principio de no discriminación. Casos C-144/04 *Werner Mangold v Rüdiger Helm*; C-555/07 *Seda Küçükdeveci v Swedex GmbH & Co. KG*; C-441/14 *Dansk Industri (DI)*, acting on behalf of *Ajos A/S v Estate of Karsten Eigil Rasmussen* y C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.*. Sin embargo, persiste una incertidumbre significativa sobre el grado en que los usuarios de servicios algorítmicos de salud pueden invocar su derecho a la igualdad conforme al Derecho de la UE.

²⁰ Véase la sentencia del Tribunal de Justicia de 17 de abril de 2018, caso C-414/16 *Egenberger*. Esta afirmación debe aplicarse a todos los motivos prohibidos por las Directivas 2000/43 y 2000/78, al igual que la discriminación por razón de religión.

Esto significa que la víctima de una decisión algorítmica discriminatoria que recibe la negativa a contratar un seguro de salud o a recibir determinada prestación sanitaria privada, más allá de los remedios que ofrece el derecho común en materia contractual, tendrá derecho a una indemnización de los daños y perjuicios sufridos como consecuencia inmediata y directa del daño ocasionado por la discriminación.²¹

3.3. LA PRUEBA DEL DAÑO MORAL

Otro de los principales problemas que surgen al aplicar la legislación antidiscriminatoria europea en el ámbito algorítmico radica en la dificultad de demostrar la existencia de una conducta discriminatoria. Se ha dicho que la opacidad de muchos algoritmos, a menudo denominados “cajas negras”, dificulta el acceso a la información sobre cómo se toman las decisiones. Esta falta de transparencia impide que las víctimas de discriminación algorítmica puedan presentar pruebas sólidas que sustenten sus reclamaciones. A lo anterior se añade la naturaleza privada de ciertos algoritmos comerciales y la consiguiente resistencia a su divulgación.

Por otra parte, la realización de la prueba basada en la comparación, inherente al derecho antidiscriminatorio, podría suponer una dificultad para los jueces a la luz de esta falta de transparencia. Para establecer la discriminación directa, los jueces suelen seleccionar comparadores reales o hipotéticos y examinar si el grupo protegido en cuestión ha recibido un trato diferencial por parte del modelo algorítmico. Dada la dificultad para probar la discriminación directa, la normativa europea permite la inversión de la carga de la prueba en determinados casos de discriminación. Este principio se recoge, como se ha avanzado más arriba, en la Directiva 2000/43/CE, art. 8, y en la Directiva 2000/78/CE, art. 9.

Según estas normas, una vez que la persona afectada aporta indicios razonables de discriminación, corresponde a la otra parte demostrar que no ha existido vulneración del principio de igualdad. Este aligeramiento de la prueba refuerza la posición de las víctimas de discriminación, facilitando su acceso a la justicia en un contexto donde la opacidad de los sistemas algorítmicos puede dificultar la obtención de evidencias. Pero, el legislador europeo ha limitado su ámbito de aplicación a los ámbitos contemplados en las referidas Directivas: a las relaciones del contrato, suministro de bienes o servicios y a determinados hechos de discriminación como el género, la raza y el origen étnico.

²¹ Sobre la discriminación algorítmica en el ámbito contractual, véase, BARBA, V. *Principio de no discriminación y contrato*. Madrid: Colex, 2023.

El Derecho español contiene normas más favorables como el art. 30 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, ya que en los casos en los que una persona alega discriminación y presenta indicios razonables, corresponde a la parte demandada demostrar que no ha habido vulneración del principio de igualdad. La Ley 15/2022 complementa así el marco normativo europeo, proporcionando una herramienta adicional para garantizar una protección efectiva contra la discriminación algorítmica, especialmente en sectores como la sanidad, donde el impacto de estos sesgos puede tener graves consecuencias y ser difícil de demostrar.

En cuanto al daño indemnizable, los perjuicios más frecuentes en el ámbito de las prestaciones de salud suelen ser los morales, en sentido estricto, y los económicos puros, ya que las decisiones discriminatorias adoptadas por los sistemas de inteligencia artificial pueden traducirse en pérdidas de oportunidades, como la imposibilidad de acceder a un determinado tratamiento o la obtención de un diagnóstico erróneo derivado de datos sesgados. Aunque el daño moral es especialmente característico en estos casos por la lesión a la dignidad de la víctima que implica toda conducta discriminatoria, se consideran indemnizables también los daños patrimoniales y los extrapatrimoniales que se deriven de la decisión discriminatoria. Sin embargo, salvo el daño moral, todos los demás perjuicios deberán probarse para que proceda su resarcimiento.

Además, el legislador proporciona una serie de criterios que deberán tenerse en cuenta para su cuantificación. Desempeñan un papel destacable en la reparación de los daños ocasionados por sistemas de inteligencia artificial las normas que ya contienen criterios de valoración del daño: el art. 9.3 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen; y el artículo 27 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que se refiere a factores de riesgo como las circunstancias del caso, la gravedad de la lesión efectivamente producida, la difusión o audiencia del medio a través del que se haya producido o la concurrencia o interacción de varias causas de discriminación. En este sentido, la referencia a la concurrencia o interacción de varias causas de discriminación permite afirmar que los casos de discriminación múltiple o interseccional merecen un mayor reproche para su autor que se traducirá en una indemnización más cuantiosa a la víctima por los perjuicios ocasionados.²² No obstante, salvo los morales, el resto de los daños no gozarán de la presunción ni de la inversión de la carga de la prueba.

²² BARBA, Principio de no discriminación, *cit.* p. 89.

En virtud del art. 27 *in fine* de la Ley 15/2022 integral de igualdad señala que: “Acreditada la discriminación se presumirá la existencia de daño moral, que se valorará atendiendo a las circunstancias del caso, a la concurrencia o interacción de varias causas de discriminación previstas en la ley y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido”.²³

Por lo que se refiere al daño moral, la mayor parte de la doctrina ha entendido que el mismo no habrá de probarse por el demandante porque se presumirá *ex lege*. La calificación de la regla del artículo 27.1 *in fine* como una presunción *iuris et de iure* es criticada por diversos motivos. En primer lugar, a falta de una expresión clara en este sentido por parte del legislador, las presunciones deberían calificarse primariamente como *iuris tantum*, según el art. 385.3 LEC. Por otra parte, la presunción *iuris et de iure* altera la función compensatoria del sistema de responsabilidad civil para transformarla en un remedio de finalidad punitiva. Por último, la reparación de las consecuencias de una discriminación no ha de pasar necesariamente por la utilización del remedio indemnizatorio: otros remedios de conducta pueden ser suficientes para eliminar todas las consecuencias de un acto discriminatorio y restaurar la situación previa a este. La redacción del artículo 27 puede llevar a los tribunales a entender que también en el caso de la concurrencia o interacción de varias causas de discriminación previstas en la ley como factor de valoración del daño la presunción ha de calificarse como *iuris et de iure* y no permitir al reclamado aportar prueba de la falta de causación de daños a pesar de haber incurrido en una conducta discriminatoria.²⁴ Estas críticas son trasladables *mutatis mutandis* a la presunción establecida en el artículo 9.3 de la LO 1/1982.

En vista de los problemas que plantea la presunción prevista en la regulación española, acaso debería revisarse la consideración de esta regla y configurarla como presunción *iuris tantum*. Las reclamaciones que pueden llegar a plantearse en relación con modelos fundacionales y con los sistemas de inteligencia artificial generativa -dado el carácter disperso y masivo de los daños potenciales- podrán ser un buen banco de pruebas para que los tribunales revisen la imposición automática de consecuencias indemnizatorias por intrusiones ilegítimas en los derechos al honor, intimidad y propia imagen.

²³ En consonancia con la regla anterior, a través de su Disposición Final 2ª se modifica la redacción del art. 217.5 LEC disponiendo dicho precepto que «En aquellos procesos en los que la parte actora alegue discriminación y aporte indicios fundados sobre su existencia, corresponderá a la parte demandada la aportación de una justificación objetiva y razonable, suficientemente probada, de las medidas adoptadas y de su proporcionalidad [...]».

²⁴ Véase BARBA, *Principio de no discriminación*, cit, p. 152.

3.4. LITIGACIÓN COLECTIVA

Pero, no se trata únicamente de garantizar la reparación de daños individuales, sino de promover cambios estructurales en el funcionamiento de las relaciones contractuales y de mercado, especialmente cuando las decisiones se toman con base en algoritmos que podrían reproducir o exacerbar sesgos preexistentes. La posibilidad de que las asociaciones y organizaciones ejerzan acciones judiciales es crucial para garantizar una protección efectiva de los derechos fundamentales y para disuadir a las empresas de implementar prácticas que vulneren los principios de igualdad y no discriminación en la Unión Europea.²⁵

En este contexto, se reconoce la legitimación activa de asociaciones y entidades representativas de colectivos potencialmente vulnerables para iniciar procedimientos judiciales en nombre de los afectados o en su apoyo. Las Directivas 2000/43/CE y 2004/113/CE exigen a los Estados miembros velar porque dichas asociaciones y organizaciones, que tengan un interés legítimo en la protección contra la discriminación, puedan intervenir, incluso a través de procedimientos colectivos, para exigir el cumplimiento de las obligaciones establecidas en las normativas específicas.

La serie de asuntos *Defrenne*, que abarcó más de una década y pidió al TJUE que se pronunciara en tres ocasiones sobre distintos aspectos del principio de igualdad de retribución, es una muestra del valor y la resistencia que pueden requerir los ciudadanos que deciden hacer valer sus derechos y los abogados que les apoyan. Esta serie de casos muestra los límites de un sistema contencioso en relación con la protección efectiva de los derechos de igualdad. Más aún, casos como el de *Defrenne* se han sometido al Tribunal en virtud del procedimiento prejudicial del artículo 267 del TFUE, que sólo da solución a casos concretos. Los casos similares, existentes y futuros, sólo se resolverán una vez que el legislador introduzca las modificaciones necesarias en la ley para introducir técnicas de litigación colectiva.

En España, el artículo 29 de la Ley 15/2002 reconoce una legitimación para la defensa del derecho a la igualdad de trato y a la de no discriminación todas las entidades y asociaciones y organizaciones representativas de los derechos de un determinado colectivo discriminado. En particular, sin perjuicio de la legitimación individual, se establece que dichas entidades pueden defender los derechos e intereses de las personas afiliadas, asociadas o usuarias de sus servicios en procesos judiciales, civiles, contenciosos,

²⁵ ZUIDERVEEN BORGESIU, F.J. “Strengthening legal protection against discrimination by algorithms and artificial intelligence”. *International Journal of Human Rights*, 2020, 24(10), 1572-1593.

administrativos y sociales, siempre que cuenten con su autorización expresa. Parece, por tanto, que se trata de una representación más que de una acción colectiva, que solo concierne al caso en que la persona discriminada actúa ante una autoridad judicial o administrativa y la entidad o asociación se persona en juicio en su lugar.

La aplicación de la legislación en materia de igualdad de género en los Estados miembros de la UE revela la existencia de otros problemas persistentes que disuaden a las personas de iniciar acciones legales para proteger su derecho a la igualdad.²⁶

En el ámbito digital, existen problemas específicos que difieren de casos más clásicos como el de *Defrenne*. Para la Sra. Defrenne no había duda de quién debía comparecer ante los tribunales por infringir el principio de igualdad salarial. Sin embargo, en relación con la discriminación algorítmica, la cuestión de los sujetos responsables puede ser más compleja, ¿debe considerarse responsable al diseñador y desarrollador de algoritmos discriminatorios o al proveedor que basa sus servicios en dichos algoritmos? Otra cuestión se refiere a la jurisdicción pertinente: ¿qué ley rige el conflicto que surge entre las víctimas de discriminación y los proveedores de productos o servicios algorítmicos y a qué tribunal debe acudir?

Como veremos en el apartado siguiente, estas cuestiones que plantean problemas para demandar civilmente a los responsables de discriminación algorítmica amparándose en la normativa antidiscriminatoria, han sido abordados por la normativa sectorial en ciernes en materia de responsabilidad por productos defectuosos y responsabilidad por daños causados por la IA.

²⁶ Estos problemas van desde dificultades institucionales (por ejemplo, la duración de los procedimientos, la falta de experiencia y asistencia, la falta de confianza en el poder judicial, la falta de compensación suficiente), problemas financieros (por ejemplo, el coste de los procedimientos, la falta de asistencia jurídica) a la incertidumbre sobre el resultado y el temor a la victimización, por parte del empleador, la familia y la sociedad. Sobre la cuestión, véase, entre otros, CHOPIN, I., CONTE, I., CHAMBRIER, E. “A comparative analysis of non-discrimination law in Europe 2018: The 28 EU Member States, the former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Montenegro, Norway, Serbia and Turkey compared (European Commission”, Luxembourg, 2019; TIMMER, A., SENDEN, “A comparative analysis of gender equality law in Europe 2018: A comparative analysis of the implementation of EU gender equality law in the EU Member States, the former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Montenegro, Norway, Serbia and Turkey”, Luxembourg, 2019.

4. APLICABILIDAD DE LA NORMATIVA SECTORIAL DE LA IA

La UE ha abordado la discriminación algorítmica tanto desde la normativa de protección de datos, como a través de la regulación de seguridad de los productos que contengan SIA. Esta normativa desarrolla los principios fundamentales de calidad de los datos y de transparencia en los algoritmos por lo que representan un avance en la materia; no obstante, persisten, como veremos, las dificultades para garantizar que los sistemas algorítmicos sean precisos, equitativos y explicables.

En este apartado se analizará tanto el marco regulatorio vigente como la normativa *in fieri*, poniendo de relieve sus virtudes y limitaciones ante los riesgos de discriminación algorítmica en el sector sanitario.

4.1. PRINCIPIOS Y REQUISITOS APLICABLES A LA SEGURIDAD DE LOS PRODUCTOS SANITARIOS CON IA

El recientemente aprobado Reglamento de Inteligencia Artificial (RIA)²⁷ tiene como finalidad la mitigación de los riesgos que conlleva dicha tecnología para la salud, la seguridad y los derechos fundamentales de las personas.

En concreto, el artículo 6.2 del RIA considera que los productos sanitarios que contengan IA son de alto riesgo. Para su regulación remite a la normativa sectorial, pero añade que los sistemas de IA de alto riesgo deben cumplir en todo caso con los requisitos referentes a la calidad de los conjuntos de datos utilizados. Deben utilizarse datos de alta calidad, suficientemente pertinentes y representativos, libres de errores y completos en vista de la finalidad del sistema, y estadísticamente adecuados según el artículo 10. Además, es necesario contar con documentación técnica actualizada y archivos de registro. Se deberá implementar un registro de actividad que permita trazar los resultados del algoritmo y conservar toda la documentación del proceso, a fin de que pueda ser evaluada por las autoridades, conforme a los artículos 11 y 12. Es fundamental garantizar la transparencia algorítmica desde el diseño y la comunicación de información a los usuarios, como establece el artículo 13. También se requiere la supervisión humana de las decisiones automatizadas, de acuerdo con el artículo 14. Finalmente, se debe asegurar la precisión, solidez y ciberseguridad del sistema, tal como indica el artículo 15.

²⁷ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

Los productos sanitarios, a su vez, se regulan en el Reglamento 2017/745,²⁸ conocido como el Reglamento de Productos Sanitarios (RPS), el cual establece un marco regulador riguroso para la autorización y supervisión de productos sanitarios, incluidos aquellos que incorporan inteligencia artificial. El Reglamento exige a los desarrolladores de algoritmos asegurarse de que sus sistemas de IA de alto riesgo queden sometidos al procedimiento de evaluación de la conformidad por parte de un organismo notificado antes de su introducción en el mercado o puesta en servicio, con el fin de demostrar que cumplen los anteriores requisitos y son altamente fiables. Para obtener la evaluación de conformidad, estos productos deben demostrar su seguridad y rendimiento a través de pruebas clínicas y evaluaciones técnicas detalladas. En especial, deben cumplir con las normas de gestión de riesgos y proporcionar evidencia de que los algoritmos utilizados no introducen sesgos o discriminación que puedan afectar negativamente a los pacientes. Una vez obtenida la certificación CE, deberán registrar dichos sistemas en una base de datos de la UE que la Comisión gestionará con el propósito de garantizar la transparencia y la vigilancia públicas y de fortalecer la supervisión *ex post* por parte de las autoridades competentes. Como novedad, el Reglamento también exige que los fabricantes implementen sistemas de gestión de calidad y mantengan una vigilancia post-comercialización monitoreando el rendimiento del producto y reportando cualquier incidente adverso con el fin de identificar y mitigar los problemas que pueda surgir una vez que el producto esté en uso.²⁹

Los referidos organismos notificados realizan una serie de evaluaciones que incluyen la revisión de la documentación técnica, auditorías de los sistemas de gestión de calidad del fabricante y, en algunos casos, inspecciones del producto una vez que ese ha sido puesto en el mercado. La profundidad y el alcance de estas evaluaciones aumenta con el nivel de riesgo del producto. Por ejemplo, los productos de Clase III, que presentan el mayor riesgo, están sujetos a las evaluaciones más rigurosas y exhaustivas. Por ello cabe plantearse en este punto la responsabilidad por evaluación de la conformidad de los organismos notificados y la responsabilidad patrimonial de las administraciones públicas en la vigilancia post comercialización.³⁰

²⁸ Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n° 178/2002 y el Reglamento (CE) n° 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo.

²⁹ Estas reglas han sido desarrolladas en España por el Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios.

³⁰ GRIMALT SERVERA, P. "La responsabilidad (civil o patrimonial) del personal médico, de los centros sanitarios y de las administraciones sanitarias por los daños causados por un producto sanitario defectuoso", *Bioderecho.es*, Núm. 17, enero-julio 2023.

Aunque, en la práctica el demandar la responsabilidad de los organismos notificados será siempre residual, se ha recurrido a este expediente en varios casos en los que el fabricante era insolvente. En Alemania³¹ y Francia³², se han presentado casos judiciales previos a la entrada en vigor del Reglamento 2017/45, en los que se analizó la responsabilidad de los organismos notificados. En el caso *Schmitt* que pertenece a la misma serie que los anteriores, el TJUE reconoció que los organismos notificados gozan de un amplio margen de discrecionalidad en la fase de vigilancia post comercialización, sin embargo, el TJUE también advirtió que este margen no debe ser ilimitado, ya que podría afectar la seguridad de los productos.³³ A partir de la entrada en vigor del Reglamento 2017/745, se introduce la obligación de realizar auditorías quinquenales sin previo aviso, lo que podría generar responsabilidad en caso de que un paciente sufriera un daño por un producto defectuoso que no hubiera sido detectado.

Respecto a la responsabilidad de las administraciones públicas, cabe mencionar el papel de la AEMPS (Agencia Española de Medicamentos y Productos Sanitarios) como organismo notificante para la certificación prevista en el Reglamento. Se ha dicho que su responsabilidad es principalmente subsidiaria, activándose solo cuando el organismo notificado no haya cumplido con sus funciones de evaluación de conformidad y el fabricante no haya adoptado las medidas correctivas necesarias. En estos casos, la AEMPS podría ser responsable si no actúa de manera oportuna y proporcional ante un riesgo grave e inminente para la salud pública. A diferencia de GRIMALT SERVERA, GARCÍA MICÓ concluye que la responsabilidad patrimonial de la AEMPS es difícil de imputar debido a la existencia de múltiples concausas en los daños que sufren los pacientes, y que su papel en la vigilancia de productos sanitarios es secundario respecto al de los organismos notificados.³⁴

4.2. LA FALTA DE TRANSPARENCIA EN LAS DECISIONES AUTOMATIZADAS

La discriminación algorítmica en el ámbito sanitario se ve agudizada por la falta de transparencia y explicabilidad en los sistemas de inteligencia artifi-

³¹ En Alemania, el BGH consideró que la responsabilidad de TÜV Rheinland debía ser tratada conforme al § 823 del BGB, concluyendo que la falta de realización de auditorías *in situ* por parte de TÜV Rheinland no se justificaba a menos que existieran indicios claros de incumplimiento. BGH NJW 2017, 2617.

³² Por su parte, la *Cour de cassation* francesa cuestionó la responsabilidad de los organismos por no ejercer facultades que tenían atribuidas, como la realización de auditorías *in situ* sin previo aviso. *Cour de cassation*, *Chambre civile 1*, 10 octobre 2018.

³³ STJUE de 16/2/2017 Caso C-219/15 (*Schmitt*/TÜV Rheinland).

³⁴ GRIMALT, La responsabilidad (civil o patrimonial) ... *op. cit.* 33; GARCÍA MICÓ, T.G. *Robótica quirúrgica y Derecho de daños*, Col.legi Notarial de Catalunya, 2024, págs. 153 y ss.

cial utilizados para la toma de decisiones automatizadas. En particular, la complejidad de las redes neuronales dificulta la detección de sesgos ocultos en los sistemas. Esta opacidad, a la que nos hemos referido como el problema de la “caja negra”, es particularmente preocupante en el contexto clínico, donde las decisiones automatizadas pueden afectar de manera significativa a la salud y el bienestar de las personas.

El Reglamento General de Protección de Datos de 2016 abordó parcialmente estos problemas, estableciendo en su artículo 13 la obligación de proporcionar “información significativa sobre la lógica aplicada” en decisiones automatizadas. No obstante, esta obligación es limitada y no garantiza el acceso a explicaciones detalladas que permitan a los afectados conocer cómo se llegó a una decisión específica ni impugnarla efectivamente.

La supervisión humana y la explicabilidad están estrechamente relacionadas, ya que la capacidad de un humano para supervisar y, si es necesario, intervenir en un sistema de IA depende en gran medida de la comprensión de cómo funciona el algoritmo. Esto implica que los sistemas de IA deben ser diseñados y operados de manera que permitan la intervención humana en cualquier momento con el fin de garantizar que las decisiones automatizadas puedan ser revisadas si se aprecia discriminación y, si es necesario, corregidas por personas.

Por dicho motivo, el artículo 22 amplía el alcance del derecho a la información reconociendo el derecho a no ser objeto de decisiones basadas únicamente en el procesamiento automatizado que produzcan efectos legales o que afecten de manera significativa al individuo. En concreto, los apartados 1 y 4 del art. 22 instauran el derecho a ser informado de la existencia de decisiones automatizadas -incluida la elaboración de perfiles-. Por su parte, el art. 22.3 consagra el derecho a la información reforzada: el interesado tiene derecho a información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.³⁵

La reciente sentencia del TJUE de diciembre de 2023 ha aclarado el alcance de esta disposición, exigiendo la intervención humana significativa en decisiones automatizadas que puedan afectar de manera importante a los individuos, estableciendo así un criterio más garantista de interpretación.³⁶

³⁵ Véase así mismo el Considerando 71, en relación al derecho a recibir una explicación sobre la decisión tomada después de un tratamiento algorítmico.

³⁶ Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 7 de diciembre de 2023, en el Caso C-634/21, sobre decisiones automatizadas y el artículo 22 del RGPD. Según esta sentencia, el artículo 22 del RGPD reconoce a los interesados el derecho a no ser sujetos a decisiones basadas únicamente en el procesamiento automatizado, incluyendo la elaboración de perfiles, que produzcan efectos legales o les afecten significativamente de manera similar. El Tribunal establece

Por su parte, el Reglamento de Inteligencia Artificial establece, como hemos visto, un marco más estricto de obligaciones para los proveedores y desplegados de sistemas de alto riesgo entre los que se encuentran los productos sanitarios (art. 6.2).

El Reglamento exige que los algoritmos sean transparentes y que los usuarios puedan entender las bases de las decisiones automatizadas. Regula, además, como veremos más adelante, la documentación técnica de los sistemas (art. 10), el registro de operaciones y la evaluación continua de la calidad y fiabilidad del sistema, con el objetivo de proporcionar un mayor grado de transparencia y evitar que los modelos de IA funcionen como cajas negras inaccesibles para las personas afectadas y las autoridades competentes.

Sin embargo, el Reglamento no contempla un derecho de acceso a esta información por parte de los individuos afectados, ni siquiera cuando se sospecha que una decisión automatizada ha producido un resultado erróneo o discriminatorio. Esto limita significativamente la posibilidad de las víctimas de acceder a información esencial para impugnar decisiones algorítmicas y solicitar reparaciones por los daños sufridos.

A lo anterior se añade la necesidad de garantizar los derechos de propiedad intelectual que pueden proteger los algoritmos. El equilibrio entre la protección de la propiedad intelectual y la necesidad de transparencia sigue siendo un problema irresuelto. El Considerando 63 del RGPD establece que la obligación de proporcionar información sobre el tratamiento automatizado no debe afectar negativamente a estos derechos, pero también especifica que no se puede denegar toda la información al interesado. No obstante, en la práctica, esta disposición se interpreta de manera restrictiva, dificultando el acceso a la información completa sobre cómo se toman las decisiones automatizadas. A su vez, el RIA se centra en garantizar la transparencia hacia las autoridades y los usuarios profesionales, ofreciendo a los individuos afectados un acceso limitado a explicaciones comprensibles, puesto que, como se ha dicho más arriba, esta regulación no está pensada para garantizar derechos

que incluso cuando una decisión se basa parcialmente en un proceso automatizado, debe haber una intervención humana significativa para cumplir con el artículo 22 del RGPD. Para superar esta prohibición de automatización, es necesario que haya una supervisión humana que pueda revisar y, si es necesario, modificar la decisión automatizada. La sentencia del TJUE tendrá implicaciones futuras para la regulación de sistemas de alto riesgo en el Reglamento de Inteligencia Artificial de la UE. El fallo podría influir en cómo se regulan estos sistemas, asegurando que se respeten los derechos de los individuos a no ser sujetos a decisiones basadas únicamente en el procesamiento automatizado. Esto podría llevar a una mayor supervisión y regulación de los sistemas de IA considerados de alto riesgo, garantizando que se implementen salvaguardias adecuadas para proteger los derechos de los usuarios.

subjetivos de los afectados por las decisiones de la SIA, sino para garantizar la seguridad de los productos.

Para abordar las referidas deficiencias, algunos expertos han propuesto la implementación de interfaces de programación de aplicaciones (API) que permitan a las autoridades, y en algunos casos a los afectados, acceder a información detallada sobre el funcionamiento de estos sistemas sin comprometer los secretos comerciales. Sin embargo, el RIA no contempla explícitamente estas soluciones, limitándose a recomendaciones generales sobre la colaboración con las autoridades competentes, lo que deja un vacío regulatorio importante que podría obstaculizar la efectiva rendición de cuentas y la protección de los derechos de los individuos.

Ante este problema, el RIA prevé medidas de apoyo, como la autorización de entornos de pruebas reglamentados (art. 53). En España, el Real Decreto 817/2023, de 8 de noviembre, crea un entorno controlado de pruebas para ensayar la aplicación de los requisitos del Reglamento Europeo de Inteligencia Artificial a los sistemas de alto riesgo. Según esta norma, el entorno permitirá a las empresas y entidades públicas probar y ajustar sus sistemas de IA en un marco regulado antes de su implementación completa.³⁷

En conclusión, a pesar de los avances que representa el RIA, la falta de acceso directo a la información detallada sobre los procesos de toma de decisiones automatizadas sigue siendo un obstáculo significativo para la protección de los derechos de los afectados especialmente en los SIA sanitarios de diagnóstico. La transparencia y la explicabilidad deben mejorarse para garantizar que las decisiones automatizadas no perpetúen las desigualdades ni afecten de manera injusta a los grupos vulnerables. Para lograr este objetivo, sería necesario un marco regulatorio más robusto que incluya una obligación de explicabilidad y acceso a los datos de entrenamiento y a las metodologías empleadas, facilitando que las personas tengan la capacidad de impugnar y obtener reparaciones por decisiones automatizadas discriminatorias en el ámbito sanitario.

4.3. EL PROBLEMA DE LA CALIDAD DE LOS CONJUNTOS DE DATOS

La calidad de los datos a partir de los cuales se diseñan y desarrollan los algoritmos de salud cobra renovada importancia a la hora de evitar o mitigar

³⁷ Véase la Exposición de Motivos del Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

la discriminación de colectivos y personas vulnerables. Tal como hemos visto más arriba, los sesgos históricos que contienen los conjuntos de datos clínicos pueden sesgar a su vez los productos sanitarios resultantes, e incluso agravar dicho sesgo. Así, la informática ha acuñado la expresión GIGO (“Garbage in, garbage out”) que se relaciona con la calidad de la información o los productos que ingresan a un sistema: si la calidad de lo que ingresa no es buena, el resultado normalmente tampoco lo es.

El RGPD no contempla de forma específica los sistemas de inteligencia artificial aunque hace referencia al requisito de calidad de los datos, requisito que debe cumplir el software sanitario.³⁸ A primera vista podría afirmarse que los principios del art. 5 RGPD revisten una importancia fundamental para el proceso de depuración de datos de cara a evitar sesgos históricos contenidos en los conjuntos de datos sanitarios, especialmente en el caso de dos principios recogidos en dicho artículo: por un lado, el requisito de minimización o limitación de los datos (art. 5.1.c) y, por otro, el requisito de exactitud de los datos (art. 5.1.d).

Sin embargo, hay que señalar que la utilidad de estos principios en relación con las aplicaciones de la IA sigue siendo dudosa, ya que, en su definición actual, no contiene requisitos técnicos específicos, sino que se limita a establecer que los datos deben ser «exactos y, en caso necesario, actualizados». Las dificultades surgen a la hora de delimitar el alcance del principio de exactitud de los datos. Según algunos estudios este principio exige un alto estándar de calidad que incluye requerimientos relativos a la exactitud, la precisión, la exhaustividad, la coherencia y la intemporalidad,³⁹ a lo que también habría que añadir la depuración de los datos para alcanzar la neutralidad o ausencia de sesgos.⁴⁰ Por el contrario, la opinión predominante es que el principio de exactitud de los datos sólo ofrece una vaga directriz general y no aborda suficientemente la calidad de los datos, por lo que debería modificarse para

³⁸ Los productos sanitarios basados en SIA deben cumplir no solo con los requisitos específicos establecidos en el referido Reglamento de Productos Sanitarios, sino que le es aplicable también el Reglamento General de Protección de Datos, en tanto estos productos se basan en datos personales. Pero, mientras que los datos de usuario en la IA médica suelen referirse a una persona concreta y, por lo tanto, son necesariamente personales (y suelen ser «sensibles» en el sentido del artículo 9 del RGPD), los datos de entrenamiento muy a menudo no sólo se seudonimizan (lo que significa que el RGPD sigue siendo aplicable según el art. 1.1, Art. 4.1 RGPD), sino que se anonimizan, de forma que el RGPD deja de ser aplicable a los datos correspondientes.

³⁹ MOEREL, L. y STORM, M. “Automated Decisions Based on Profiling: Information, Explanation or Justification – That Is The Question!” *Autonomous Systems and the Law* Editors: Nikita Aggarwal, Horst Eidenmüller, Luca Enriques, Jennifer Payne, Kristin van Zwieten. Beck C. H., 2019, 1-11.

⁴⁰ STÖGER, SCHNEEBERGER, KIESEBERG, HOLZINGER, “Legal aspects of data cleansing in medical AI” *Computer Law & Security Review* 42 (2021) 105587.

incluir requisitos más detallados.⁴¹ Procede señalar en este punto que, a diferencia del RGPD, la Directiva 2016/680 relativa a infracciones penales ofrece requisitos más detallados sobre la calidad de los datos,⁴² lo que parece indicar que el legislador europeo no quería crear normas detalladas sobre la calidad de los datos en el RGPD.⁴³

En segundo lugar, se ha apuntado que el principio de exactitud de los datos puede entrar en conflicto con el principio de limitación de los datos. Para garantizar los derechos del interesado, cumplir con el principio de minimización de datos, es decir, recopilar y transferir los datos que sean absolutamente necesarios para la finalidad declarada, es de suma importancia en un entorno de uso intensivo de datos para el aprendizaje automático. Téngase además en cuenta que, de acuerdo con el principio de responsabilidad (art. 5. 2 RGPD), el responsable del tratamiento debe poder demostrar el cumplimiento de ambos principios, y que ambos sirven como técnica de referencia en la privacidad por diseño contemplada en el art. 25 del RGPD. Sin embargo, el principio de limitación de los datos y, en especial, la estricta prohibición relativa al tratamiento de datos sensibles (art. 9.1 RGPD) limitan la recopilación de suficientes datos de entrenamiento de alta calidad y, por tanto, la precisión de los sistemas de IA.⁴⁴

A lo anterior hay que añadir que, en algunas situaciones, la recopilación de datos especialmente sensibles puede ser necesaria para las necesidades de entrenamiento con el fin de evitar que el sistema de lugar a decisiones discriminatorias.⁴⁵ El Reglamento de Inteligencia Artificial establece al respecto en su art. 10.5 una excepción a la prohibición de tratar datos sensibles si el tratamiento es estrictamente necesario para garantizar el control, la detección y la corrección de sesgos siempre que se apliquen las salvaguardias adecuadas, lo que permite

⁴¹ HACKER, “A Legal Framework for AI Training Data” (2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598; HOEREN, “Thesen zum Verhältnis von Big Data und Datenqualität” *Multimedia und Recht*, (2016) 19, 8.

⁴² Art. 7 apartado 2 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de estos datos, y por la que se deroga la Decisión marco 2008/977/JAI del Consejo [2016] DO L119/89.

⁴³ STÖGER *et al.* Legal aspects of data cleansing in medical AI *op. cit.*, p. 67.

⁴⁴ GOODMAN, “B. Discrimination, Data Sanitisation and Auditing in the European Union’s General Data Protection Regulation”, *European Data Protection Law Review*, Volume 2, Issue 4 (2016), pp. 493 - 506.

⁴⁵ ŽLIOBAIT y CUSTERS, ‘Using Sensitive Personal Data May be Necessary for Avoiding Discrimination in Data-driven Decision Models’ *AI and Law* (2016) 24 183; KLEINBERG, LUDWIG, MUL-LAINATHAN y SUNSTEIN, “Discrimination in the Age of Algorithms” *Journal of Legal Analysis* (2018) 10 174; WILLIAMS, BROOKS y SHMARGAD, “How Algorithms Discriminate Based on Data They Lack” *Journal of Information Policy* (2018) 8 78.

salvar, al menos en teoría, la objeción apuntada en relación a los datos de entrenamiento que requieren los dispositivos médicos que funcionan con SIA.⁴⁶

Además, el art. 10 establece que cuando se emplean técnicas que implican el entrenamiento de modelos de IA, se considera preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos de entrenamiento, validación y prueba sean de buena calidad.⁴⁷ Este conjunto de previsiones es aplicable a los productos sanitarios con inteligencia artificial, además de las previsiones del Reglamento 2017/745.

Sin embargo, pese a las mejoras introducidas por el RIA, la doctrina ha puesto de relieve que las normas referidas siguen adoleciendo de una gran inconcreción. Faltan desarrollos normativos específicos de lo que se conside-

⁴⁶ El art. 10.5 del Reglamento 2024/1689 establece que: “En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas”. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes: a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos; b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización; c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas; d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos; e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior; f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

⁴⁷ Por su parte, el Considerando 44 desarrolla el estándar refiriéndose específicamente a los datos sesgados: «Los conjuntos de datos de entrenamiento, validación y prueba deben ser lo suficientemente pertinentes y representativos, carecer de errores y ser completos en vista de la finalidad prevista del sistema. Asimismo, deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los grupos de personas en las que en un principio se usará el sistema de IA de alto riesgo. En concreto, los conjuntos de datos de entrenamiento, validación y prueba deben tener en cuenta, en la medida necesaria en función de su finalidad prevista, los rasgos, características o elementos particulares del entorno o contexto geográfico, conductual o funcional específico en el que se pretende utilizar el sistema de IA. Con el fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial, para garantizar que el sesgo de los sistemas de IA de alto riesgo se vigile, detecte y corrija».

ra alta calidad del conjunto de datos que minimice el riesgo de resultados discriminatorios.⁴⁸

4.4. LA RESPONSABILIDAD POR DAÑOS MORALES CAUSADOS POR LA IA

La responsabilidad por daños morales causados por la IA es un tema complejo. Hemos mencionado anteriormente que los daños provocados por la discriminación algorítmica plantean retos significativos en cuanto a su atribución y compensación, debido a la opacidad inherente de muchos sistemas de IA y a la dificultad de probar la causalidad.

En este contexto, tanto en el derecho europeo como en el español, la responsabilidad extracontractual derivada de los daños causados por sistemas de inteligencia artificial en el ámbito sanitario, especialmente en lo que se refiere a daños morales, sigue siendo un área poco definida. La falta de claridad en la legislación actual agrava los desafíos ya mencionados, subrayando la necesidad de un marco jurídico más robusto y específico.

a) Propuesta de Directiva de Responsabilidad por Productos Defectuosos

La Propuesta de Directiva de Responsabilidad por Productos Defectuosos (PDRPD)⁴⁹ pretende revisar la vigente Directiva 85/374/CEE para adaptarla al contexto digital ampliando su ámbito de aplicación al uso de IA en productos de consumo y dispositivos médicos.

La propuesta amplía la definición del concepto de producto para incluir los componentes de software (art. 4). Además, establece una presunción de defecto y causalidad cuando se demuestra que el producto no cumple con los requisitos de seguridad, facilitando la imputación de responsabilidad en casos de fallos de diseño o errores algorítmicos que resulten en decisiones discriminatorias (art. 8).

La PDRPD también extiende la responsabilidad a las actualizaciones y modificaciones de software realizadas tras la venta del producto (art. 10), reconociendo que los sistemas de IA pueden evolucionar tras su comercialización y que los defectos pueden introducirse en etapas posteriores, generando riesgos adicionales para los usuarios.

⁴⁸ Existen certificaciones sin valor normativo que abordan la calidad de los datos y la minimización del sesgo en sistemas de IA. Una de las más destacadas es la ISO/IEC 42001:2023, que establece un marco para los Sistemas de Gestión de Inteligencia Artificial (SGIA). Esta norma proporciona directrices para asegurar que los sistemas de IA sean fiables, transparentes y éticos. ISO/IEC 42001:2023(en) Information technology - Artificial intelligence - Management system.

⁴⁹ Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre responsabilidad por los daños causados por productos defectuosos. COM/2022/495 final.

Aunque la propuesta de Directiva reconoce los daños psicológicos comprobados médicamente como daños personales compensables (art. 12), se centra principalmente en los daños materiales y personales, incluyendo la pérdida o destrucción de datos (art. 6), dejando fuera los daños morales como la discriminación algorítmica⁵⁰. La propuesta remite a la normativa de los Estados miembros en lo que atañe a la compensación por este tipo de daños.

Por tanto, la Directiva no cubre ni los daños morales *stricto sensu*, ni los daños económicamente puros, que precisamente son los que con mayor frecuencia se producen cuando se vulnera este derecho fundamental a través de un sistema algorítmico de toma de decisiones. Siendo así, es preciso constatar que, aunque esta propuesta representa un avance significativo en la regulación de la responsabilidad por los daños causados por la IA en la Unión Europea, sigue presentando importantes lagunas en relación con la compensación por daños morales respecto de los cuales tampoco en esta ocasión habrá armonización.

b) Propuesta de Directiva sobre Responsabilidad Civil por Daños Causados por la IA

La propuesta de Directiva sobre Responsabilidad Civil por Daños Causados por la IA (PDRC) tiene como objetivo armonizar la normativa sobre responsabilidad en los Estados miembros, facilitando la reclamación de daños causados por la IA, incluidas las situaciones de discriminación algorítmica.⁵¹

⁵⁰ En el considerando 18 de la PDRPD se establece que los Estados miembros «deben ofrecer una indemnización completa y adecuada por todas las pérdidas materiales derivadas de la muerte, o de lesiones corporales, o los daños o la destrucción de bienes y la pérdida o corrupción de datos, las normas para calcular la indemnización deben ser establecidas por los Estados miembros. Además, la presente Directiva no debe afectar a las normas nacionales relativas a los daños morales».

Por consiguiente, según la citada Propuesta, dentro de la definición de «daños» quedan comprendidas: «las pérdidas materiales resultantes de: a) muerte o lesiones corporales, incluidos los daños para la salud psicológica comprobados médicamente; b) daños o destrucción de cualquier propiedad, excepto: i) el propio producto defectuoso; ii) un producto dañado por un componente defectuoso de ese producto; iii) las propiedades utilizadas exclusivamente con fines profesionales; c) pérdida o corrupción de datos que no se utilicen exclusivamente con fines profesionales» (art. 4.6 de la PDRPD).

Al cubrir las pérdidas materiales debidas a la pérdida, destrucción o corrupción de datos, la propuesta reconoce la importancia de los datos en la era digital. Sin embargo, la propuesta no va más allá de lo “necesario” y, por tanto, no aborda otros tipos de daños, como la privacidad o la discriminación. En suma, la protección de los consumidores exige una indemnización por las pérdidas materiales derivadas no sólo de la muerte o las lesiones corporales, como los gastos funerarios o médicos o la pérdida de ingresos, y de los daños materiales, sino también de la pérdida o corrupción de datos. La Propuesta no afecta a la indemnización por infracciones de otras normas, tales como el RGPD.

⁵¹ Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA) COM/2022/496 final.

La propuesta introduce un régimen de responsabilidad objetiva para los sistemas de IA de alto riesgo (art. 5), lo que implica que los operadores pueden ser considerados responsables de los daños causados por sus sistemas sin necesidad de probar negligencia o *mala praxis*, siempre que se acredite la existencia de un daño y su relación con el SIA. Esta previsión se aplica a los productos sanitarios que son considerados de alto riesgo por la RIA y por la normativa sectorial. Para facilitar la carga de la prueba a las víctimas de los daños ocasionados por estos sistemas, se presumirá *iuris tantum* la causalidad en determinadas circunstancias (art. 4).⁵²

Aunque la Directiva no aborda específicamente la compensación por daños morales, deja abierta la posibilidad de que los Estados miembros incluyan estos daños en sus legislaciones internas (art. 6), ya que, se trata de una Directiva de mínimos que permite a los Estados miembros «adoptar o mantener normas nacionales más favorables para que los demandantes fundamenten sus demandas civiles de responsabilidad extracontractual por daños y perjuicios causados por sistemas de IA, siempre que dichas normas sean compatibles con el Derecho de la Unión» (art. 1.4).

Esta disposición será particularmente relevante para los casos de discriminación algorítmica, porque permite la aplicación de las normas sobre inversión de la carga de la prueba prevista en el artículo 4, además de la presunción sobre la existencia de daños morales prevista en el art. 27 de la Ley 15/2022 integral de igualdad, una vez acreditada la discriminación.⁵³

5. CONCLUSIONES

El creciente uso de la inteligencia artificial en el sector sanitario ha dado lugar a casos de discriminación algorítmica que provocan efectos graves en la atención médica, reproduciendo o incluso intensificando las desigualdades estructurales existentes. Los sesgos presentes en los datos y en el diseño de los modelos algorítmicos pueden traducirse en desventajas significativas para grupos protegidos, comprometiendo así la equidad en el acceso y la calidad de los servicios de salud.

⁵² Sobre esta cuestión, véase NAVAS NAVARRO, S. “Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial”, *Cesco*, N° 44/2022.

⁵³ BERENGUER ALBALADEJO, M^a C. “La discriminación algorítmica en la toma de decisiones individualizadas: qué es, por qué se produce y cuáles son los principales desafíos que plantea”, *Revista de Derecho Privado*, núm. 6, noviembre-diciembre 2023, págs. 45 y ss.

La normativa existente en la Unión Europea, a saber el Reglamento General de Protección de Datos (RGPD) y el reciente Reglamento de Inteligencia Artificial (RIA), proporcionan un marco inicial para la mitigación de riesgos a través de la regulación de la calidad de los datos y de la obligación de supervisión humana cuando se trata de productos de alto riesgo, como es el caso de los productos sanitarios; no obstante, estas disposiciones aún presentan limitaciones significativas en cuanto a su efectividad para abordar la opacidad de los sistemas y la complejidad de los procesos de toma de decisiones automatizadas.

Un aspecto clave a considerar es la responsabilidad derivada de la implementación de sistemas de IA en el ámbito sanitario, especialmente en aquellos casos donde se generen daños que no se encuentren vinculados a una relación contractual preexistente entre las partes.

Las reglas de derecho antidiscriminatorio europeo establecen la inversión de la carga de la prueba contemplada en Directivas como la 2000/43/CE y la 2000/78/CE. Esta regla se convierte en una herramienta clave para las víctimas, facilitando su acceso a la justicia en contextos donde la opacidad de los sistemas algorítmicos dificulta la obtención de pruebas concluyentes. Acreditada la existencia de discriminación, las víctimas no tienen que probar el daño en sí mismo, sino que el demandado debe demostrar que el algoritmo no es discriminatorio o que el daño no deriva de su uso. En este contexto, la regla de armonización mínima que adoptan las Directivas permite que los demandantes de daños causados por sistemas de IA invoquen normas más favorables del Derecho nacional y no cabe duda de que, en materia de no discriminación, la norma más beneficiosa sería la que contempla la inversión de la carga de la prueba de la Ley 15/2022 integral de igualdad en relación con el art. 217.5 LEC, disposición que además es compatible con el futuro Derecho de la Unión en materia de responsabilidad de la inteligencia artificial.

En lo que respecta a la prueba de los daños derivados de la discriminación, el artículo 27 de la Ley 15/2022 establece una norma favorable al perjudicado, ya que, una vez acreditada la discriminación, se presume la existencia de daño moral, que será valorado atendiendo a las circunstancias del caso, a la concurrencia o interacción de varias causas de discriminación previstas en la ley y a la gravedad de la lesión efectivamente producida, considerando, en su caso, la difusión o audiencia del medio a través del cual se haya perpetrado. Por lo tanto, en cuanto al daño moral, no será necesario que el demandante lo pruebe, ya que se presumirá *ex lege*. Además, el legislador proporciona una serie de criterios que deben ser tenidos en cuenta para su cuantificación. La referencia a la “concurrencia o interacción de varias causas de discriminación” permite concluir que los casos de discriminación múltiple o intersec-

cional merecen un mayor reproche para su autor, lo que se traducirá en una indemnización superior para la víctima por los perjuicios ocasionados.

Por su parte, la normativa sectorial *in fieri* contiene algunas previsiones en materia de responsabilidad extracontractual de los SIA sanitarios. Así, la propuesta de Directiva sobre responsabilidad civil de la IA tiene un ámbito de aplicación más amplio que la propuesta de Directiva de productos defectuosos y permite la reclamación de cualquier tipo de daño o perjuicio cubierto por la legislación nacional, incluidos aquellos derivados de la discriminación. También abarca cualquier tipo de víctima, ya sean particulares, empresas u organizaciones. No obstante, las víctimas deben recurrir a las normas nacionales en materia de responsabilidad para reclamar una indemnización, aunque la propuesta de Directiva sobre responsabilidad en materia de IA podría facilitar estas reclamaciones mediante las medidas que contempla.

La propuesta introduce un régimen de responsabilidad objetiva para los sistemas de IA de alto riesgo (art. 5), lo que implica que los operadores pueden ser considerados responsables de los daños causados por sus sistemas sin necesidad de probar negligencia o *mala praxis*, siempre que se acredite la existencia de un daño y su relación con el SIA. Esta previsión se aplica a los productos sanitarios que son considerados de alto riesgo por la RIA y por la normativa sectorial. Para facilitar la carga de la prueba a las víctimas de los daños ocasionados por estos sistemas, se presumirá *iuris tantum* la causalidad en determinadas circunstancias (art. 4), entre las cuales está que el demandante pruebe que el resultado arrojado por el sistema IA le ha causado daños comprobables.

Como conclusión, podemos decir que la normativa europea de responsabilidad civil para la IA y la normativa española de igualdad de trato y no discriminación se complementan en sus objetivos y mecanismos de protección. La normativa española proporciona una protección específica en cuanto a la inversión de la carga de la prueba de discriminación, mientras que la normativa sectorial europea introduce principios de responsabilidad objetiva y facilita las reclamaciones en casos de daños por IA de alto riesgo. En el sector sanitario será preciso recurrir a este marco facilitador para la protección de los afectados por discriminación algorítmica.

No obstante, los remedios jurídicos para la discriminación algorítmica deben estar orientados no solo a la reparación de daños individuales, sino a la prevención de sesgos sistemáticos que perjudiquen de manera desproporcionada a determinados colectivos. Es fundamental que el diseño e implementación de sistemas algorítmicos integre principios de equidad desde sus etapas iniciales, promoviendo prácticas de auditoría continua y supervisión externa que aseguren un control efectivo. La transparencia y la explicabilidad de los

algoritmos constituyen, en este sentido, pilares fundamentales para restaurar la confianza pública y garantizar una responsabilidad clara frente a los efectos discriminatorios.

Además, las herramientas de mitigación deben incluir mecanismos de evaluación de impacto específicos para la sanidad, que consideren no solo los riesgos individuales, sino también los potenciales efectos agregados sobre poblaciones vulnerables. La creación de órganos de supervisión, como la Agencia Española de Supervisión de la Inteligencia Artificial, constituye un paso en la dirección correcta para monitorear y regular el uso de la IA, aunque su efectividad dependerá de la capacidad de estas instituciones para ejercer una vigilancia activa y de la colaboración estrecha con otros agentes del sistema sanitario.

En suma, aunque el panorama normativo europeo ha avanzado en la conceptualización y abordaje de la discriminación algorítmica en el sector sanitario, queda un largo camino por recorrer si se quieren evitar los riesgos de discriminación existentes. Es necesario impulsar reformas legislativas que aborden de manera específica las particularidades de los sistemas de IA aplicados a la salud, así como fomentar la adopción de buenas prácticas que aseguren la equidad y no discriminación. Solo a través de un enfoque integral que combine la innovación tecnológica con un marco regulatorio robusto, podremos garantizar que la inteligencia artificial en el ámbito sanitario sea una herramienta segura, inclusiva y equitativa.

La armonización del tratamiento legal de la responsabilidad civil contractual y extracontractual del metaverso con la regulación europea sobre plataformas en línea

CRISTINA ARGELICH COMELLES

*Profesora Ayudante Doctor de Derecho civil
Universidad Autónoma de Madrid*

Sumario: 1. Consideraciones iniciales acerca del Metaverso y la responsabilidad civil. 2. Identidad digital del responsable civil y propiedad de los activos digitales patrimoniales. 3. El régimen de responsabilidad del proveedor de servicios de la plataforma y del usuario profesional en el ordenamiento jurídico europeo. 3.1. La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad civil contractual: hacia un sistema de responsabilidad civil objetiva por pérdida o desprogramación de un activo digital y por discriminación algorítmica. 3.2. La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad extracontractual por los daños causados en las plataformas del Metaverso. 4. Reflexiones prospectivas sobre la responsabilidad civil contractual y extracontractual: el informe español para la Comisión Europea en materia de contratación con inteligencia artificial.

1. CONSIDERACIONES INICIALES ACERCA DEL METAVERSO Y LA RESPONSABILIDAD CIVIL

Para abordar la naturaleza jurídica del Metaverso, un acrónimo formado por el prefijo “meta-”, que significa más allá, y el sustantivo “universo”, no

encontramos un concepto actual y completo del Metaverso, que integre el *hardware* y su interacción entre la realidad digital y el mundo real. Por ello, definimos el Metaverso como la red de mundos virtuales en tres dimensiones, a modo de traslación de Internet al mundo real como realidad digital, y centrados en la conexión social con el usuario mediante su *hardware*: la realidad aumentada y su interacción con auriculares y gafas de realidad aumentada, la realidad mixta, la realidad virtual, y las tecnologías de la realidad digital¹. Estas se componen de: la tecnología *blockchain*, para la automatización de las decisiones previamente programadas; Web3 o el Internet operado mediante tecnología *blockchain*, cuyo contenido es inmutable e incensurable, y no se puede hackear ni colgar; y los sistemas de inteligencia artificial o IA para la toma autónoma de decisiones.

En consecuencia, la naturaleza jurídica que le corresponde al Metaverso es la propia de la Tierra virtualizada como realidad digital, porque a ella se vincula, aunque pueda operar paralelamente. Calificarla así permite que los abusos tengan el tratamiento legal propio de la realidad material, con las adaptaciones que requiera para su aplicación en este entorno digital, algo especialmente relevante en materia de responsabilidad civil extracontractual por los daños causados en el Metaverso. La tecnología que requiere el Metaverso se compone del *hardware*, como la realidad aumentada, la realidad mixta y la realidad virtual, junto con las tecnologías de la realidad digital, consistentes en la tecnología *blockchain* y Web3, así como el *software* pertinente.

Hechas estas precisiones iniciales y por lo que respecta a la estructura del presente trabajo, se analizará la propiedad de los activos digitales alojados en las plataformas en línea, también las del Metaverso, como son un ejemplo los *in-game digital assets*, para seguidamente abordar la identidad digital del responsable civil. Tras ello, se examinará el régimen de responsabilidad del proveedor de servicios de la plataforma en línea y del usuario profesional en el ordenamiento jurídico europeo para incardinar posteriormente la responsabilidad civil contractual por incumplimiento, debiendo destacar la pérdida o desprogramación de los activos digitales y por discriminación algorítmica como ejemplos de la insuficiencia del régimen de responsabilidad actual, y la responsabilidad civil extracontractual por los daños causados en el Metaverso.

¹ ARGELICH COMELLES, C. (2022). El Derecho civil ante el Metaverso: hacia un Metalaw europeo y sus remedios en el Multiverso. *Derecho digital e innovación*, 12, 1-26.

2. IDENTIDAD DIGITAL DEL RESPONSABLE CIVIL Y PROPIEDAD DE LOS ACTIVOS DIGITALES PATRIMONIALES

Tras la aprobación del Reglamento 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE², conocido como eIDAS, se ha evolucionado de la firma electrónica a la identidad digital con el Reglamento 1183/2024 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital³. La identidad digital va a facilitar la mejora de la seguridad en la autenticación en las plataformas en línea. Además, permitirá enlazar dicha identidad digital a la representación gráfica del usuario y, por ende, vincularle el régimen de responsabilidad civil correspondiente. No obstante, el principal reto jurídico se sitúa en el tratamiento legal del procesamiento automático de los datos de carácter personal⁴, en atención al régimen de responsabilidad por dicho procesamiento ilegal de datos, fijado por el Tribunal de Justicia de la Unión⁵.

En el ámbito de la Unión Europea, los criptoactivos encuentran su regulación en el Reglamento 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos 1093/2010 y 1095/2010 y las Directivas 2013/36/UE y 2019/1937⁶, conocido como Reglamento MiCA, que establece obligaciones para los emisores y proveedores de servicios de criptoactivos, así como en la regulación establecida para los mercados e instrumentos financieros en la Directiva MiFID II y el Reglamento MiFIR. En este sentido, encontramos diversos tipos de criptoactivos que examinaremos⁷, a saber: las criptomonedas, las *stablecoins* y las divisas digitales controladas por un Banco Central; los

² DOUE de 28 de agosto de 2014.

³ DOUE de 30 de abril de 2024.

⁴ WALSH, P. (2020). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention 108. Digital Identities. Council of Europe, 1-24, <https://rm.coe.int/tpd-2020-04rev-digital-identity-tc-en/1680a0c051.%20/>.

⁵ STJUE de 5 de marzo de 2024, ECLI:EU:C:2024:202.

⁶ DOUE de 9 de junio de 2023. FETSYAK SENKIV, I. (2024). Impacto de la Propuesta de Reglamento de prevención de blanqueo de capitales en las transacciones con criptoactivos. ¿El fin de las «wallet» sin custodia y de las transacciones «crypto» anónimas?, *Diario La Ley*, 10487, 1-5.

⁷ KRYSA, F. (2023). Taxonomy and Characterisation of Crypto Assets in Private International Law. En BONOMI, A., LEHMANN, M., LALANI, S., (eds.), *Blockchain and Private International Law*, Leiden, Brill, 157-208. PARRONDO, L. (2023). Cryptoassets: Definitions and accounting treatment under the current International Financial Reporting Standards framework. *International Journal of Intelligent Systems in Accounting and Finance Management*, 4, 1-20.

tokens no fungibles; y los *security tokens*, vinculados a inversiones financieras o a la Tokenización de bienes u otros activos.

En primer lugar, las criptomonedas son instrumentos de pago carentes de soporte físico, que se basan en un algoritmo y el registro electrónico donde se almacenan. Es necesario precisar que se trata de un algoritmo matemático, como lo son la mayoría, y que no está entrenado con Inteligencia Artificial a los efectos de que su funcionamiento sea cambiante, como sucede en los *dynamic pricing algorithms*, por ejemplo. Encontramos también las *stablecoins*, es decir, una criptomoneda de cotización estable y cuya operatividad radica en la facilitación de pagos e intercambios en el extranjero, evitando las variaciones en los tipos de cambio por los pagos en divisas diferentes. Para concluir con los cryptoactivos, es necesario referirse a las *Central bank digital currencies*, conocidas como CBDCs, y referidas a una moneda digital que representa la divisa controlada y emitida por un Banco Central, como lo será en un futuro el Euro digital o EURM, que actualmente está en fase de pruebas.

En segundo lugar, encontramos los *non-fungible tokens* o NFTs, es decir, un token que representa la propiedad de un activo digital único e individualizado -por tanto, no fungible y cuya transmisión se sujeta al régimen jurídico de las obligaciones específicas-, a modo de certificado al *tokenholder* como propietario y que le faculta para su disposición. Asimismo, el token en los NFTs también puede utilizarse para probar la identidad de su titular, para tokenizar la transmisión de la propiedad con trazabilidad de la operación, así como para probar la propiedad de ítems virtuales en videojuegos y plataformas en línea, como los avatares -tokenizados-, las fincas virtuales o los *in-game digital assets*. Separadamente, encontramos los *security tokens*, utilizados como ficha de seguridad para una inversión financiera, como acciones o bonos, así como obras de arte⁸, y también para la Tokenización de activos reales o digitales.

Habida cuenta de lo expuesto, los activos digitales se programan de la siguiente manera: la representación gráfica es *online*, y la programación de sus metadatos se encuentra *on-chain*. Por tanto, los activos digitales no tienen un activo real vinculado, lo que incide en su tratamiento legal respecto de la Tokenización de bienes⁹. A modo de ejemplo divulgativo, la representación gráfica y los metadatos de los NFTs corresponderían a un objeto y su código de

⁸ LACRUZ MANTECÓN, M. L. (2023). Propiedad Intelectual y tecnología inteligente. *Revista Crítica de Derecho Inmobiliario*, 99(800), 3103-3146.

⁹ NASARRE AZNAR, S. (2020). Naturaleza jurídica y régimen civil de los “tokens” en “blockchain”. En GARCÍA TERUEL, R. M. (coord.), *La tokenización de bienes en blockchain: cuestiones civiles y tributarias*, Cizur Menor, Thomson Reuters Aranzadi, 61-108. GARCÍA-TERUEL, R. M., SIMÓN-MORENO, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, 41, 1-16. ARRIETA SEVILLA, L. J. (2023). El uso de tokens en transmisiones inmobiliarias. *Revista de Derecho Civil*, X(2), 71-116.

barras en la realidad material, respectivamente. Un código de barras permite la identificación del bien, pero no impide su transformación no autorizada, ni la pérdida de la cosa debida o la imposibilidad sobrevenida de la prestación; en el entorno digital, este último supuesto tendrá lugar mediante la desprogramación del activo digital. En consecuencia, debido a su existencia *online* y *on-chain*, lo único que es posible trasladar de un activo digital a la realidad material es el almacenamiento de una copia de su representación gráfica, como archivo, no como activo, y cuya calificación jurídica será la de dato.

Respecto del uso de los activos digitales patrimoniales en la realidad material¹⁰, los criptoactivos se podrán utilizar remotamente mediante las *cryptowallets*, a modo de cartera virtual. En este sentido, las criptomonedas son aceptadas como método de pago en diversas plataformas en línea, e incluso cabe canjear su saldo disponible en métodos de pago como *PayPal*, en este caso, respecto de la criptomoneda *Bitcoin*. Por otra parte, los *NFT wallets* permiten almacenar la información sobre la ubicación de los NFTs en la plataforma donde se alojan los metadatos, así como adquirir nuevos NFTs, al tiempo que aseguran la interoperabilidad agrupando los NFTs coleccionables ubicados en diversas plataformas.

3. EL RÉGIMEN DE RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE LA PLATAFORMA Y DEL USUARIO PROFESIONAL EN EL ORDENAMIENTO JURÍDICO EUROPEO

El régimen jurídico de las plataformas en línea, también aplicable a las que conforman el Metaverso, se distribuye en diversos Reglamentos europeos, a saber: el Reglamento 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea¹¹, en adelante, *P2B Regulation*; el Reglamento 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales¹²), en adelante, DSA; y el Reglamento 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre merca-

¹⁰ SCHULLER, R. R. (2022). Criptoactivos. Categorización jurídica de los criptoactivos e introducción a la tecnología DLT/Blockchain. *Cuadernos de Derecho Transnacional*, 14(2), 737-769. PACHECO JIMÉNEZ, M. N. (2022). De la digitalización de los pagos a los tokens del metaverso. *La Ley mercantil*, 91, 1-20.

¹¹ DOUE de 11 de julio de 2019.

¹² DOUE de 27 de octubre de 2022.

dos disputables y equitativos en el sector digital y por el que se modifican las Directivas 2019/1937 y 2020/1828 (Reglamento de Mercados Digitales¹³), en adelante, DMA.

En el estudio elaborado para el Parlamento Europeo, de 5 de febrero de 2021, denominado *Liability of online platforms*¹⁴, se examinan las principales alternativas regulatorias ante la responsabilidad de las plataformas en línea: mantener el estado de la cuestión; la sensibilización acerca de su utilización; la promoción de la autorregulación; el establecimiento de herramientas de coregulación; la adopción de normativa estatutaria sobre la responsabilidad de las plataformas; y la modificación de la responsabilidad de las plataformas en línea, mediante las condiciones para la exención de responsabilidad o el establecimiento de un régimen armonizado de responsabilidad.

A este respecto, es oportuno indicar que los algoritmos no son neutrales, pues algunos utilizan la IA, como lo relativos al *pricing*, y su programación puede tener sesgos humanos. Todo ello conduce a un eventual resultado discriminatorio en la elección final del consumidor en las plataformas en línea. En el ámbito de las plataformas en línea, la discriminación algorítmica puede producirse de diversas maneras¹⁵, pues la formación del algoritmo se divide en tres fases: *process level*, *model level* y *classification level*. En la fase *process level*, el *machine learning* mediante el que el algoritmo se forma y adapta al entorno puede contener datos sesgados, que alteren materialmente su neutralidad teórica. En la fase *model level*, ello obedece a que los datos originarios son parciales o incorrectos, lo que se soluciona mediante un tratamiento de datos adecuado del *Big Data*; esto es, lo que se conoce como *cleaning the data*, o que dichos datos se encuentren vinculados a una discriminación estructural. En la fase *classification level*, ello sucede cuando, en la selección de unas determinadas características del consumidor o factores relativos al producto, se ocasiona la discriminación que la propia plataforma pretende, por ejemplo, porque el *target* de clientes de un determinado producto deba reunir unas características. En el Derecho del consumo no disponemos, ni en los Estados Unidos ni en el Derecho de la Unión, de una regulación relativa a la discriminación algorítmica que articule remedios para mitigar sus efectos.

¹³ DOUE de 12 de octubre de 2022.

¹⁴ EUROPEAN PARLIAMENT (2021). *Liability of online platforms*, European Parliamentary Research Service, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU\(2021\)656318_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf).

¹⁵ WHITTAKER, M., CRAWFORD, K., DOBBE, R., FRIED, G., *et. al.* (2018). *AI Now Report*, European Commission, Futurium, 1-63, https://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf. KROLL, J., HUEY, J., BAROCAS, S., FELTEN, E., *et. al.* (2017). *Accountable Algorithms*. *University of Pennsylvania Law Review*, 165, 633-705, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

Por todo ello, mientras no se aborde una regulación en materia de discriminación algorítmica omnicomprendensiva, tendremos que encomendarnos a la autorregulación de las plataformas en línea mediante los mecanismos reputacionales, así como los eventuales *Corporate Compliance* de las empresas a las que se vinculan, para atender materialmente la protección del consumidor en este ámbito. Así, será posible proporcionar información acerca del tratamiento de los datos vertidos en la plataforma, la información de los derechos acerca de su tratamiento, las obligaciones de la plataforma al respecto, el acceso a los mismos y su confidencialidad, y las acciones de los poderes públicos al respecto. No obstante, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE¹⁶ -en adelante RGPD- solo se refiere a datos de carácter personal; ello excluye el *machine learning* y los datos personales que sean necesarios para evitar la discriminación en las materias en las que ha sido regulada. En suma, la regulación algorítmica omnicomprendensiva que debería abordarse pasa, de momento, por la autorregulación en las plataformas en línea.

Por lo que respecta al régimen jurídico aplicable a las plataformas en línea, analizaremos brevemente los Reglamentos europeos indicados. El examen de la *P2B Regulation* tendrá carácter tangencial, por referirse a la relación jurídica entre una plataforma y un empresario, por tanto, B2B; en este caso, entre un usuario profesional respecto de una plataforma intermediaria en línea, habitualmente bajo la figura del contrato de distribución. Sin embargo, su importancia es indubitable, pues constituye el primer antecedente normativo para pasar de la autorregulación de las plataformas a su normativización en el contexto del mercado único europeo. Respecto de los algoritmos y la protección del consumidor, se encuentra una referencia expresa a los algoritmos en el art. 5.6: a los efectos de establecer los parámetros principales que rigen la clasificación de los productos o servicios en las plataformas en línea, no se exigirá a los proveedores de los servicios de intermediación en línea ni a los proveedores de los motores de búsqueda la revelación de los algoritmos que puedan inducir a error a los consumidores, o bien causarles un perjuicio mediante la manipulación de los resultados.

En cuanto a la prevención de la discriminación algorítmica en los contratos de consumo, la DSA se fundamenta en tres objetivos específicos en el art. 1: la protección efectiva de los consumidores y sus derechos fundamentales en las plataformas en línea; el establecimiento de la transparencia y responsabilidad de estas plataformas; y la promoción de la innovación, el crecimiento y la

¹⁶ DOUE de 4 de mayo de 2016.

competitividad en el mercado único europeo. La *P2B Regulation* se enfoca en la transparencia y los remedios privados en las relaciones B2B, mientras que la DSA atribuye responsabilidad al proveedor de la plataforma cuando preste el servicio, salvo por las causas de exoneración de los arts. 4-6, como hemos explicado. Complementariamente, se ha creado el Observatorio de la Unión Europea sobre la economía de las plataformas en línea para examinar las últimas tendencias en este tema, en relación con la Recomendación de la Unión Europea 2018/334, de 1 de marzo de 2018, sobre medidas para abordar de manera efectiva los contenidos ilegales en línea, también regulada en el art. 8 DSA.

La DSA confirma el principio de responsabilidad limitada de los intermediarios en línea, pues no se produce una ampliación de la responsabilidad civil. El fundamento de este régimen de responsabilidad se encuentra en las *asymmetric due diligence obligations* u obligaciones asimétricas de diligencia debida que deben cumplir las autoridades competentes. Las obligaciones de diligencia debida se sustentan, a su vez, en la transparencia y el *platform procedure* o procedimiento de plataforma, como por ejemplo la notificación y tramitación de reclamaciones, la solución extrajudicial de controversias, los mecanismos reputacionales e incluso la incorporación del *Corporate Compliance*. Con este enfoque en cuestiones de procedimiento, la DSA sigue la tendencia reciente de una “procedimentación” de la regulación de la plataforma, como se había venido produciendo mediante la autorregulación con los mecanismos reputacionales, así como en la *P2B Regulation*. En este sentido, debemos mencionar que en las *Model Rules on Online Platforms*¹⁷ del *European Law Institute* se incide en las cuestiones clave en materia de responsabilidad de las plataformas en línea, como son la falta de transparencia, la influencia de la plataforma sobre el proveedor y la falta de diligencia. Finalmente, para las *very large online platforms* o grandes plataformas en línea, el art. 33 DSA aporta una nueva forma de regulación sectorial para plataformas sistémicamente importantes. Este enfoque se basa en la regulación de los servicios financieros con diversas obligaciones de cumplimiento. Deberemos atender a si las obligaciones de presentación de informes y auditoría son suficientes para garantizar un “entorno en línea seguro, confiable y transparente”, como exige la DSA.

En cuanto a la DMA, el objetivo es conseguir que las plataformas en línea de gran tamaño actúen de forma justa en su actividad, con los criterios objetivos de su calificación como guardián de acceso contenidos en los arts. 1 y 3: tener una posición económica sólida, un impacto significativo en el mer-

¹⁷ EUROPEAN LAW INSTITUTE (2019). *Model Rules on Online Platforms*, https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

cado interior y estar activo en varios Estados de la Unión Europea; tener una fuerte posición intermediaria al vincular una pluralidad de usuarios a diversas empresas; y tener una posición consolidada en el mercado. La DMA garantiza la equidad de los términos y condiciones de las plataformas en línea al establecer las prácticas comerciales desleales de los guardianes de acceso en su art. 5. La DMA también mejora la oferta al consumidor y permite que las plataformas se ocupen de nuevos servicios. En caso de incumplimiento de las normas establecidas, se establece un régimen sancionador de hasta el 10% de la facturación anual de la empresa, así como otros remedios y sanciones tras una investigación de la plataforma. Finalmente, el tratamiento legal de la transparencia algorítmica en la DMA se concreta en su examen y el régimen de responsabilidad, el papel de los algoritmos en la economía y sociedad digital junto con la gobernanza de datos, así como los códigos de conducta, en relación con el *Corporate Compliance* y los mecanismos reputacionales.

3.1. LA INCARDINACIÓN DEL RÉGIMEN JURÍDICO DE LAS PLATAFORMAS EN LÍNEA EN LA RESPONSABILIDAD CIVIL CONTRACTUAL: HACIA UN SISTEMA DE RESPONSABILIDAD CIVIL OBJETIVA POR PÉRDIDA O DESPROGRAMACIÓN DE UN ACTIVO DIGITAL Y POR DISCRIMINACIÓN ALGORÍTMICA

A los efectos de apreciar la pérdida o destrucción de la cosa, los activos digitales no se pueden deteriorar, sino que solamente se pueden desprogramar de la plataforma donde se almacenen sus metadatos. Dicha desprogramación obedecerá a dos causas: por el cumplimiento de las obligaciones establecidas en la normativa europea sobre plataformas en línea, o bien por un “hackeo” o ataque informático al registro electrónico que contiene los metadatos del activo digital. Por una parte, la desprogramación del proveedor de servicios de la plataforma en línea, en cumplimiento de las obligaciones de suspensión y terminación del servicio de un usuario profesional en caso de afectación a los derechos de terceros, en virtud de los arts. 4 y 5 de la *P2B Regulation*, le exoneran de responsabilidad en los arts. 4-6 DSA, siendo responsable el usuario profesional frente al titular o consumidor del activo digital.

Respecto de la pérdida del activo digital en atención a lo expuesto, conviene referir el caso “Metabirkins” o la transformación no autorizada en NFTs del bolso *Birkin* de la firma *Hermès* por parte del usuario profesional *Metabirkins*, así como su comercialización indebida en diversas plataformas en línea. En el caso *Hermès Int’l v. Rothschild*, enjuiciado por el Tribunal Federal de Nueva York el pasado 2 de febrero de 2023, se establece que dicha comercialización correspondería a la firma *Hermès* o mediante su transformación autorizada,

por lo que condenó a la parte demandada a pagar 130.000 dólares en concepto de indemnización por daños y perjuicios¹⁸. Por otra parte, la pérdida del activo digital puede producirse por un “hackeo” o ataque informático, quedando el proveedor de la plataforma habilitado para reprogramar el activo digital. El “hackeo” ocasiona un *bug* o falla en la *blockchain* que hace que no se pueda autoejecutar lo programado, por lo que el único remedio informático es la reprogramación desde el *hash* anterior a este *bug*, para que así se autoejecute la cadena más larga. Los casos de los *crypto panics* ilustran bien lo expuesto, pues cuando se produce dicho ataque informático, la única solución es su reprogramación.

Complementariamente y en materia de errores de programación y hackeos, el MIT Media Lab¹⁹ señala que los *hackers* se han apropiado del equivalente a 1.800 millones de dólares en criptomonedas. Ello se debe a los *bugs* o errores en el programa informático de las plataformas correspondientes. En particular, no referimos a los fallos en la plataforma *Ethereum*, conocidos como el ataque a *The DAO*²⁰ de 2016 y el ataque a *Parity*, junto con otros casos a los que nos remitimos²¹. Estos errores en la programación derivan del automatismo de la tecnología *blockchain* y, en consecuencia, de su irreversibilidad, porque no se puede detener su ejecución sino solamente revertir sus efectos mediante la reprogramación. Ningún código informático está exento de *bugs*, lo que requiere su comprobación previa en aras de evitar resultados inadecuados y garantizar su ejecución sin intervención humana o reprogramación. Estos errores conllevan el incremento de la inversión para evitarlos y de los costes de indemnización por una programación defectuosa. Por ello, apuntamos que una extensión del Metaverso mediante las plataformas en las que opera debería llevar aparejada una responsabilidad de carácter objetivo de la plataforma, mediante la aceptación de los términos y condiciones de uso de esta, siendo especialmente útil en caso de un error de programación en la plataforma. Asimismo, dicha aceptación debería llevar aparejada la formaliza-

¹⁸ *Hermes Int'l v. Rothschild*, 22-cv-384 (JSR) (S.D.N.Y. Feb. 2, 2023), <https://casetext.com/case/hermes-intl-v-rothschild-9>. Cuestión distinta es el reciente y sorprendente pronunciamiento acerca de la creación de NFTs sobre obras pictóricas, cuyo titular es la firma Mango, en el que se ha autorizado la transformación en estos activos digitales aun no siendo esta firma la autora de las obras pictóricas. Véase la SJM Barcelona de 11 de enero de 2024, ECLI:ES:JMB:2024:1.

¹⁹ ORCUTT, M. (2019). Once hailed as unhackable, blockchains are now getting hacked. *MIT Technology Review*, <https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/>.

²⁰ ATZEL, N., BARTOLETTI, M., CIMOLI, T. (2017). A survey of attacks on Ethereum smart contracts. *Proceedings of the 6th International Conference on Principles of Security and Trust*, 10204, 1-23.

²¹ Estos casos se refieren a *CoinDash ICO*, con una pérdida en criptomonedas de 10 millones de dólares, la Estafa del Proyecto Enigma, consistente en una venta falsificada de *Tokens* que supuso una pérdida de 1.500 *Ethers*, el robo de *Tether*, que perdió el equivalente a 31 millones en *Tokens*, y la Estafa de Bitcoin Gold, que conllevó una pérdida del equivalente a 3 millones de dólares.

ción de un contrato de seguro que cubriese los daños generados al adherente, sin tener que demostrar nada más que el perjuicio económico.

La pérdida digital del activo y su posible reprogramación tiene una incidencia directa en la extinción de las obligaciones por destrucción de la cosa, de conformidad con el art. 1156 CC, así como en el uso de activos digitales como garantía real, en la línea de los *ELI Principles on the Use of Digital Assets as Security*²², del European Law Institute, en adelante *ELI Principles*. La existencia de los activos digitales patrimoniales necesita la preservación de la *blockchain* en la que se almacenan sus metadatos, está condicionada a que no se produzca su desprogramación, y no le afecta la transmisión de carteras de activos digitales entre plataformas -incluyendo la sucesión de empresa- o su interoperabilidad, comprendiendo las *crypto wallets*, porque permanece su programación. En este sentido, presenta poca utilidad una propiedad digital que no sea interoperable, y ello requiere un diseño armonizado de la interfaz gráfica del usuario o GUI en las distintas plataformas en línea, siguiendo las obligaciones de accesibilidad de la DSA. Del mismo modo y en la línea de los *ELI Principles*, si se ha constituido una garantía real sobre un activo digital, solamente cabrá extinguirla por el cumplimiento de la obligación principal, además de por su desprogramación. En caso de desprogramación, se eliminan estos activos digitales de la plataforma, pero su constancia previa quedará registrada por la inmutabilidad del registro distribuido; en el entorno *off-chain*, en caso de pérdida o destrucción de un bien, será necesaria su cancelación registral. En atención a lo expuesto, no será posible calificar de pérdida del activo digital el olvido de las claves de acceso, pues la plataforma tendrá alojados los datos y, mediante los procedimientos que establezca, será posible recuperar las claves de acceso; tras la sucesión, debería establecerse la obligación al proveedor de la plataforma de facilitar a los herederos el acceso a la cuenta privada del causante y sus claves, si no se contienen expresamente en el testamento.

Por lo que respecta a la responsabilidad contractual establecida en la regulación europea sobre plataformas en línea -referida a la DSA, la DMA, y la *P2B Regulation*- el responsable civil será el usuario profesional frente al titular de los activos digitales. Solo responderá el proveedor de servicios de la plataforma por infracción de las obligaciones de diligencia debida o por haber realizado prácticas anticompetitivas -ateniéndose al régimen administrativo sancionador dispuesto para estas cuestiones respectivamente en la DSA y la DMA²³-, así como cuando haya efectuado una actividad de intermediación y

²² EUROPEAN LAW INSTITUTE (2022). *ELI Principles on the Use of Digital Assets as Security*, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf.

²³ WIELSCH, D. (2019). Private Law Regulation of Digital Intermediaries. *European Review of Private Law*, 27(2), 197-220. TERESZKIEWICZ, P. (2018). Digital Platforms: Regulation and

no concurra en las causas de exoneración de responsabilidad, dispuestas en los arts. 4-6 DSA en atención a la falta de relación de causalidad. Precisamos que, en atención al referido art. 6 DSA y en cumplimiento del art. 4 *P2B Regulation*, el proveedor de servicios de la plataforma también se exonera de responsabilidad por la suspensión o terminación del servicio de un usuario profesional, en el supuesto de afectación a los derechos de terceros, como en el referido caso de los *Metabirkins*.

Este régimen de responsabilidad civil contractual de las plataformas en línea es insuficiente, al menos, en los siguientes casos: por desprogramación de un activo digital -por un “hackeo” o por la vulneración de los derechos de terceros-, por colusión algorítmica -como práctica anticompetitiva parcialmente regulada en la *P2B Regulation* y la DMA-, y por discriminación algorítmica, carente de tratamiento legal específico. Por ello, a los efectos de evitar que el usuario profesional no responda como debe ante el consumidor y titular del activo digital desprogramado, y teniendo en cuenta que la *P2B Regulation*, la DSA y la DMA se van a modificar, -como ya se indicaba durante la tramitación de estos dos últimos, ante la escasa aplicación práctica del primero-, sería conveniente reformular esta responsabilidad en términos de *strict liability* o *semi-strict liability*, como se contiene en el estudio para el Parlamento Europeo *Liability of Online Platforms* y en la línea de lo aludido por la doctrina europea²⁴, ante la insuficiencia de las obligaciones de diligencia debida y el régimen administrativo sancionador.

A modo de reflexión prospectiva, los retos que plantea el Metaverso a los consumidores de activos digitales afectan principalmente a la protección de datos de carácter personal, referidos al control de identidad y los ficheros de

Liability in the EU Law. *European Review of Private Law*, 26(6), 903-920. RODRÍGUEZ DE LAS HERAS BALLELL, T. (2014). Refusal to Deal, Abuse of Right and Competition Law in Electronic Markets and Digital Communities. *European Review of Private Law*, 22(5), 685-702. MONTERO PASCUAL, J. J. (2024). *El reglamento de mercados digitales. La regulación de las grandes plataformas*, Valencia, Tirant lo Blanch, 113-255. BUESO GUILLÉN, P. J. (2023). Aproximación a las novedades en el derecho de defensa de la competencia de la Unión Europea en el tratamiento del uso de Internet por el distribuidor autorizado en los sistemas de distribución selectiva. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales*, Barcelona, Atelier, 259-280. HERRERO SUÁREZ, C. (2023). Merger control in digital markets: don't trust the trusts. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales*, Barcelona, Atelier, 227-239.

²⁴ EUROPEAN PARLIAMENT (2021). *Liability of online platforms*, European Parliamentary Research Service, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU\(2021\)656318_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf). CAUFMANN, C., GOANTA, C. (2021). A New Order: The Digital Services Act and Consumer Protection, *European Journal of Risk Regulation*, 1(1), 1-17. BÜYÜKSAGIS, E. (2022). Extension of Strict Liability to E-Retailers. *Journal of European Tort Law*, 13(1), 64-86. FROSIO, G. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review*, 112, 19-46.

solvencia, así como a los controles que les asisten como consumidores, debiendo destacar el control de transparencia. Ante los nuevos escenarios que pueden derivarse de la implementación de las nuevas tecnologías en la contratación B2C en las plataformas en línea, el control de incorporación es el único de los controles que asisten al consumidor cuya regulación actual sería suficiente, porque su cumplimiento podría comprobarse en dos estadios: *ab initio*, con la incorporación de las Condiciones Generales de la Contratación y la aceptación expresa del consumidor, mediante el “*I agree button*”, de los términos y condiciones de uso de la plataforma correspondiente; y, durante su formación, a través la tecnología *blockchain*, que permite el cruce automático de información entre distintas instituciones para comprobar si las Condiciones Generales han sido incorporadas al contrato de manera transparente, para permitir su perfección. El ajuste legal del control de contenido, referido a las condiciones generales, y el control de transparencia de las condiciones particulares del contrato, por su componente subjetivo, pasa necesariamente por la regulación del papel que la IA y los algoritmos tengan en el *machine learning* de la plataforma y en los términos y condiciones de uso de esta, para adaptar la protección del consumidor atendiendo a la transparencia material del contrato.

3.2. LA INCARDINACIÓN DEL RÉGIMEN JURÍDICO DE LAS PLATAFORMAS EN LÍNEA EN LA RESPONSABILIDAD EXTRA CONTRACTUAL POR LOS DAÑOS CAUSADOS EN LAS PLATAFORMAS DEL METAVERSO

Finalmente, en materia de responsabilidad civil extracontractual por los daños causados en las plataformas en línea inmersivas -en particular, las que conforman el Metaverso-, debemos armonizar la responsabilidad contractual de las plataformas con el régimen jurídico de la responsabilidad civil extracontractual. En atención a lo expuesto, la responsabilidad civil extracontractual por los daños causados en estas plataformas debería seguir también el sistema de responsabilidad objetiva referido en el estudio, en este caso, por el riesgo de la actividad, fundamentándolo en las siguientes razones: la manifiesta insuficiencia de las obligaciones de diligencia debida para disciplinar al proveedor de servicios de la plataforma; la dificultad para identificar y localizar al agente del daño sin la colaboración de la plataforma; y que el daño se produce en una plataforma creada y mantenida por su proveedor, que debe ofrecer un entorno digital seguro al usuario.

Apostar en este entorno por la responsabilidad civil subjetiva o por hecho propio, *ex art.* 1902 CC, plantea dos problemas: la prueba de la relación de causalidad, también aplicable a este contexto, al que se añade la difícil iden-

tificación y localización efectiva del agente del daño sin el establecimiento de una obligación legal de colaboración del proveedor de servicios de la plataforma, que necesariamente pasa por las obligaciones de diligencia debida de la responsabilidad civil por hecho ajeno. Por el contrario, un sistema de responsabilidad objetiva garantiza la necesaria disciplina del proveedor de servicios de la plataforma, pudiendo moderar su alcance: con una responsabilidad *fault-based system* según consta en el estudio-, por ejemplo, por desprogramación del activo digital, por discriminación algorítmica, así como por los daños de carácter material o físico; con un sistema de *semi-strict liability*, correspondiente con nuestro sistema de responsabilidad por hecho ajeno por incumplimiento del deber de diligencia, por ejemplo, respecto de la colaboración aludida, advirtiendo de la falta de coercibilidad por las causas de exoneración de los arts. 4-6 DSA; o bien una responsabilidad civil objetiva por riesgo de la actividad o *strict liability*, que implicaría la cobertura de la responsabilidad por todo daño causado en estas plataformas.

El inconveniente que plantea el establecimiento de un sistema de responsabilidad objetiva absoluta o pura es la asunción de los costes de su aseguramiento obligatorio, pudiendo ser sufragados por vía de publicidad en la plataforma o mediante el pago de unas *fees* a cargo del usuario, lo que puede suponer su disminución, salvo que pueda monetizar su actividad en la plataforma. El establecimiento de un sistema de responsabilidad objetiva puede conllevar que algunas plataformas dejen de operar en la Unión, pudiendo restringir la exigencia de esta responsabilidad a las grandes plataformas en línea y los guardianes de acceso, en consonancia con los deberes agravados para estas plataformas previstos en la DSA y la DMA, respectivamente.

4. REFLEXIONES PROSPECTIVAS SOBRE LA RESPONSABILIDAD CIVIL CONTRACTUAL Y EXTRA CONTRACTUAL: EL INFORME ESPAÑOL PARA LA COMISIÓN EUROPEA EN MATERIA DE CONTRATACIÓN CON INTELIGENCIA ARTIFICIAL

En este apartado, se formulan unas observaciones prospectivas en materia de responsabilidad civil contractual y extracontractual en materia de contratación automatizada, contratación con inteligencia artificial y contratos algorítmicos -referidos al uso de asistentes digitales-, a la luz del informe nacional de España emitido en autoría individual para la Comisión Europea en el estudio “*Novel forms of contracting in the digital economy*”, respecto de los contratos de consumo y entre empresarios. Con carácter previo, es necesario indicar que las vías para regular la IA apuntadas por diversos académicos europeos serían

las siguientes: la prohibición de las decisiones totalmente automáticas, del art. 22 RGPD; la inclusión de un *algorithmic impact assessment*, del art. 35 RGPD, para la evaluación obligatoria de los algoritmos que afecten a derechos y libertades individuales; la monitorización y auditoría de los algoritmos; una regulación con remedios privados frente a la responsabilidad civil; y una regulación pactada entre las autoridades y las plataformas.

Considerando la responsabilidad civil por el uso de un sistema de IA proporcionado por un tercero para la contratación²⁵, la responsabilidad contractual implica un acuerdo mediante una licencia o servicio *ex art.* 1107 CC, que incluye la responsabilidad civil del proveedor de la IA por los errores causados por la IA en la contratación, y la responsabilidad extracontractual concierne al proveedor de la IA integrada en un determinado sistema, según el art. 1902 CC.

Con respecto a la responsabilidad contractual por el uso de un sistema de IA en la contratación, tal y como recomiendan los Principios 2 y 6 del Informe Provisional del *European Law Institute* “*EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?*”²⁶, se debe proteger al consumidor por el uso de un asistente digital, considerando también la responsabilidad civil por falta de conformidad prevista en el art. 117 TRLGDCU. En este sentido, cabe mencionar que la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por productos defectuosos²⁷ protegerá a las personas físicas, incluidos los consumidores según los arts. 135 y 137 TRLGDCU, por los daños físicos y materiales causados por un sistema de IA, independientemente de si se proporciona dicho sistema en virtud de un contrato.

El tratamiento legal de la responsabilidad extracontractual de la IA integrada en un determinado sistema debe remitirse a la responsabilidad civil subjetiva o por hecho propio del art. 1902 CC, al no estar regulada en el ámbito de la responsabilidad por hecho ajeno prevista en los arts. 1903-1910 CC, ni en

²⁵ MARTÍN CASALS, M. (2023). Las Propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, 3, 55-100, <https://indret.com/wp-content/uploads/2023/07/1806.pdf>. YZQUIERDO TOLSADA, M. (2001). *Sistema de responsabilidad contractual y extracontractual*, Madrid, Dykinson, 1-545. PANTALEÓN PRIETO, F. (1991). El sistema de responsabilidad contractual. *Anuario de Derecho Civil*, 44(3), https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1991-30101901092,1019-1092.

²⁶ EUROPEAN LAW INSTITUTE (2023). *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?*, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

²⁷ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por productos defectuosos, COM/2022/495 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>.

la legislación especial respecto de la responsabilidad objetiva. Por lo que respecta al requisito de la relación de la causalidad del art. 1902 CC, la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial²⁸ contiene una presunción *iuris tantum* de relación de causalidad en la responsabilidad civil subjetiva, prevista en el art. 4, de modo que el proveedor de un sistema de IA podría ser considerado responsable. En cuanto a la negligencia del contratante que utiliza la IA, la legislación española podría adaptarse para mantener la inversión de la carga de la prueba en el contexto de la responsabilidad subjetiva o por hecho propio, e incluso establecer un régimen de responsabilidad objetiva del proveedor de la IA.

BIBLIOGRAFÍA

- ARGELICH COMELLES, C. (2022). El Derecho civil ante el Metaverso: hacia un Metalaw europeo y sus remedios en el Multiverso. *Derecho digital e innovación*, 12, 1-26.
- ARRIETA SEVILLA, L. J. (2023). El uso de tokens en transmisiones inmobiliarias. *Revista de Derecho Civil*, X(2), 71-116.
- ATZEI, N., BARTOLETTI, M., CIMOLI, T. (2017). A survey of attacks on Ethereum smart contracts. *Proceedings of the 6th International Conference on Principles of Security and Trust*, 10204, 1-23.
- BUESO GUILLÉN, P. J. (2023). Aproximación a las novedades en el derecho de defensa de la competencia de la Unión Europea en el tratamiento del uso de Internet por el distribuidor autorizado en los sistemas de distribución selectiva. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales*, Barcelona, Atelier, 259-280.
- BÜYÜKSAGIS, E. (2022). Extension of Strict Liability to E-Retailers. *Journal of European Tort Law*, 13(1), 64-86.
- CAUFMANN, C., GOANTA, C. (2021). A New Order: The Digital Services Act and Consumer Protection, *European Journal of Risk Regulation*, 1(1), 1-17.
- EUROPEAN LAW INSTITUTE (2019). *Model Rules on Online Platforms*, https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

²⁸ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, COM/2022/496 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496>.

- EUROPEAN LAW INSTITUTE (2022). *ELI Principles on the Use of Digital Assets as Security*, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf.
- EUROPEAN LAW INSTITUTE (2023). *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?*, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.
- EUROPEAN PARLIAMENT (2021). *Liability of online platforms*, European Parliamentary Research Service, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU\(2021\)656318_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf).
- FETSYAK SENKIV, I. (2024). Impacto de la Propuesta de Reglamento de prevención de blanqueo de capitales en las transacciones con criptoactivos. ¿El fin de las «wallet» sin custodia y de las transacciones «crypto» anónimas?, *Diario La Ley*, 10487, 1-5.
- FROSIO, G. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review*, 112, 19-46.
- GARCÍA-TERUEL, R. M., SIMÓN-MORENO, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, 41, 1-16.
- HERRERO SUÁREZ, C. (2023). Merger control in digital markets: don't trust the trusts. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales*, Barcelona, Atelier, 227-239.
- KROLL, J., HUEY, J., BAROCAS, S., FELTEN, E., *et. al.* (2017). Accountable Algorithms. *University of Pennsylvania Law Review*, 165, 633-705, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.
- KRYSA, F. (2023). Taxonomy and Characterisation of Crypto Assets in Private International Law. En BONOMI, A., LEHMANN, M., LALANI, S., (eds.), *Blockchain and Private International Law*, Leiden, Brill, 157-208.
- LACRUZ MANTECÓN, M. L. (2023). Propiedad Intelectual y tecnología inteligente. *Revista Crítica de Derecho Inmobiliario*, 99(800), 3103-3146.
- MARTÍN CASALS, M. (2023). Las Propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, 3, 55-100, <https://indret.com/wp-content/uploads/2023/07/1806.pdf>.
- MONTERO PASCUAL, J. J. (2024). *El reglamento de mercados digitales. La regulación de las grandes plataformas*, Valencia, Tirant lo Blanch.
- NASARRE AZNAR, S. (2020). Naturaleza jurídica y régimen civil de los “tokens” en “blockchain”. En GARCÍA TERUEL, R. M. (coord.), *La tokenización de bienes en blockchain: cuestiones civiles y tributarias*, Cizur Menor, Thomson Reuters Aranzadi, 61-108.

- ORCUTT, M. (2019). Once hailed as unhackable, blockchains are now getting hacked. *MIT Technology Review*, <https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/>.
- PACHECO JIMÉNEZ, M. N. (2022). De la digitalización de los pagos a los tokens del metaverso. *La Ley mercantil*, 91, 1-20.
- PANTALEÓN PRIETO, F. (1991). El sistema de responsabilidad contractual. *Anuario de Derecho Civil*, 44(3), https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1991-30101901092, 1019-1092.
- PARRONDO, L. (2023). Cryptoassets: Definitions and accounting treatment under the current International Financial Reporting Standards framework. *International Journal of Intelligent Systems in Accounting and Finance Management*, 4, 1-20.
- RODRÍGUEZ DE LAS HERAS BALLELL, T. (2014). Refusal to Deal, Abuse of Right and Competition Law in Electronic Markets and Digital Communities. *European Review of Private Law*, 22(5), 685-702.
- SCHULLER, R. R. (2022). Criptoactivos. Categorización jurídica de los criptoactivos e introducción a la tecnología DLT/Blockchain. *Cuadernos de Derecho Transnacional*, 14(2), 737-769.
- TERESZKIEWICZ, P. (2018). Digital Platforms: Regulation and Liability in the EU Law. *European Review of Private Law*, 26(6), 903-920.
- WALSHE, P. (2020). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention 108. Digital Identities. Council of Europe, 1-24, <https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc-en/1680a0c051.%20/>.
- WHITTAKER, M., CRAWFORD, K., DOBBE, R., FRIED, G., *et. al.* (2018). *AI Now Report*, European Commission, Futurium, 1-63, [tps://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf](https://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf).
- WIELSCH, D. (2019). Private Law Regulation of Digital Intermediaries. *European Review of Private Law*, 27(2), 197-220.
- YZQUIERDO TOLSADA, M. (2001). *Sistema de responsabilidad contractual y extracontractual*, Madrid, Dykinson.

Transparencia y explicabilidad para prevenir la discriminación de los sistemas de inteligencia artificial: la interacción entre el RGPD y el RIA¹

M^a CRISTINA BERENGUER ALBALADEJO

*Profesora Titular de Derecho civil
Universidad de Alicante*

Sumario: 1.- LA DISCRIMINACIÓN ALGORÍTMICA COMO UNO DE LOS PRINCIPALES RIESGOS DERIVADOS DEL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA TOMA DE DECISIONES; 2.- LA OPACIDAD COMO PRINCIPAL ESCOLLO PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA; **2.1 Consideraciones previas; 2.2 Opacidad en el uso y sobre el contenido de los algoritmos; 2.3. Opacidad jurídica y técnica del algoritmo;** 3.- TRANSPARENCIA ALGORÍTMICA Y EXPLICABILIDAD: ¿QUÉ IMPLICAN ESTAS EXIGENCIAS?; 4.- MEDIDAS PARA GARANTIZAR LA TRANSPARENCIA Y LA EXPLICABILIDAD EN LA TOMA DE DECISIONES ALGORÍTMICAS; **4.1 Estado de la cuestión; 4.2. La transparencia y la explicabilidad en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de protección de datos (RGPD): especial referencia a las decisiones automatizadas del art. 22; 4.2.1. Ámbito de aplicación del art. 22 RGPD; A) Excepciones; B) La prohibición general del art. 22 RGPD: presupuestos de aplicación a la luz de la última jurisprudencia del TJUE en su sentencia de 7 de diciembre de 2023; 4.2.2. Contenido del derecho de información de los arts. 13.2 g), 14.2 g) y 15.1 h); 4.3. La transparencia y la explicabilidad en el Reglamento**

¹ Trabajo realizado al amparo del Proyecto de Investigación «La irrupción de la inteligencia artificial en el Derecho de daños y su adaptación a las nuevas tecnologías», referencia PID2020-116185GB-I00 (Ministerio de Ciencia e Innovación - Agencia Estatal de investigación) y del Proyecto «La nueva era de los algoritmos y la inteligencia artificial y su tutela jurídico-privada en el marco de la Unión Europea», referencia CIPROM/2022/40 (Programa Prometeo para Grupos de Investigación de Excelencia 2023 de la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital).

(UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de IA; 4.3.1 Obligaciones de transparencia y comunicación de información; A) Sistemas de alto riesgo; B) Determinados sistemas de IA con independencia de su riesgo; 4.3.2 Derecho a una explicación; 5. CONSIDERACIONES FINALES SOBRE LA NECESIDAD DE TRANSPARENCIA Y EXPLICABILIDAD PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA.

1. LA DISCRIMINACIÓN ALGORÍTMICA COMO UNO DE LOS PRINCIPALES RIESGOS DERIVADOS DEL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA TOMA DE DECISIONES

Se ha definido la discriminación algorítmica como aquella que se produce cuando un individuo o grupo recibe un tratamiento arbitrario o injusto como consecuencia de la toma de decisiones automatizadas². La principal diferencia con la discriminación que podríamos llamar «analógica» es la forma de llevarla a cabo, en tanto que la primera implica el uso de algoritmos y también, usualmente, de tecnología inteligente. No obstante, la conducta discriminatoria sería idéntica en ambos casos siempre que la decisión adoptada (bien por el humano, bien por el sistema de inteligencia artificial -en adelan-

² Así, MERCADER UGUINA, J.R. «Discriminación algorítmica y derecho granular: nuevos retos para la igualdad en la era del big data», *Labos: Revista de Derecho del Trabajo y Protección Social*, vol. 2, n. 2, 2021, p. 6. Con más detalle la define CASTILLO OCARANZA, C., «Discriminación algorítmica en el ámbito laboral», en P. Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, p. 72, para quien existe discriminación algorítmica cuando un «algoritmo o sistema computacional algorítmico (X) produce discriminación grupal para una persona (Y) respecto de otra (Z), es decir, produce un resultado peor para la persona (Y) respecto a la persona (Z) debido a que (Y) pertenece a un cierto grupo social saliente o «socially salient group» (entendiendo por tal, aquél que pueda ser fácilmente identificado y que sea tal que pertenecer o no a este grupo tenga consecuencias para las relaciones sociales, y en particular, las relaciones de poder -ej. grupos delimitados por género, etnia, raza, discapacidad etc). Además, (X) debe haber basado su decisión en una observación estadísticamente relevante, es decir, en cualquier información que (X) utilice basándose en los datos de entrada (ej. si un empleador no contrata a una persona por tener la característica de ser mujer -que es un grupo social saliente- y contrata a otra que no es mujer basándose en la observación estadística de que es más probable que una mujer pida una baja por maternidad». Otras definiciones de este fenómeno se recogen en: FERNÁNDEZ DE LA MORENA, B., *Discriminación algorítmica. Estudio del sesgo en arquitecturas de aprendizaje profundo*, UAM, Madrid, 2019, p.1; CASTELLANOS CLARAMUNT, J., «Derecho e inteligencia artificial: atención especial a los sesgos, la privacidad y la protección de datos», accesible en <https://idpbarcelona.net/derecho-e-inteligencia-artificial-atencion-especial-a-los-sesgos-la-privacidad-y-la-proteccion-de-datos/>, la define como «un fenómeno que se produce cuando sistemas de IA o algoritmos utilizados para tomar decisiones automatizadas discriminan de manera indirecta o inconsciente a ciertas personas o grupos»; o GINÉS i FABRELLAS, A., «Sesgos discriminatorios en la automatización de decisiones en el ámbito laboral: evidencias de la práctica», en RIVAS VALLEJO, P. (dir), *Discriminación algorítmica en el ámbito laboral*, Navarra, 2022, p. 302.

te, IA-) diera lugar a un trato diferente e injusto en situaciones comparables, o a un trato idéntico en situaciones distintas, basado en motivos protegidos y sin que hubiese justificación objetiva y razonable para ello³.

Se ha destacado reiteradamente por las instituciones y la doctrina que uno de los mayores riesgos del uso de los sistemas de IA es la adopción de decisiones sesgadas y discriminatorias que, además de afectar a las personas concretas objeto de la decisión, lleven a reproducir y perpetuar estereotipos y desigualdades contra los que se lleva siglos luchando. Desde la *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL))*, hasta el reciente *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, RIA)*⁴, ha sido constante el reconocimiento de que el derecho fundamental a la igualdad de trato y la no discriminación, junto con el de protección de datos personales y la intimidad, son especialmente vulnerables a través de esta tecnología y merecedores de una tutela especial, aumentado el riesgo de que sean vulnerados de forma proporcional al grado de autonomía del sistema utilizado, ya que el humano puede llegar a perder la dirección y control sobre las decisiones adoptadas, sin que además se pueda llegar a saber en base a qué motivos el sistema decide de una manera determinada⁵. De hecho, el peligro de que los sistemas de IA puedan perpetuar

³ CONSEJO DE EUROPA, *Manual de legislación europea contra la discriminación* (edición 2018), Luxemburgo, 2019, p. 46 y ss. Los denominados «motivos» o «características protegidas» son aquellas condiciones de la persona que no se deben considerar relevantes para administrarle un trato diferenciado u otorgarle un determinado beneficio. Tanto es así, que no cualquier desigualdad de trato conlleva discriminación prohibida sino sólo la basada en tales características o motivos. Vid., ARCOS VARGAS, M., «La no discriminación en el Derecho derivado de la Unión Europea» en J.M. MORALES ORTEGA (dir.), *Realidad social y discriminación. Estudios sobre diversidad e inclusión laboral*, Murcia, 2022, pp. 26 y ss.

⁴ DOUE de 12 de julio de 2024.

⁵ Otros documentos que recogen esta idea son, entre otros muchos, el *Libro Blanco sobre Inteligencia artificial*, de 19 de febrero de 2020, p. 13, donde se mencionan los riesgos de la IA para los derechos fundamentales en general, haciendo especial referencia a la protección de los datos personales y a la no discriminación; la *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))*, que concibe la discriminación como una de las posibles causas en la producción de «lesión o daño» por estas tecnologías en el artículo 4 del Reglamento que la acompaña, estando presente en toda la propuesta el derecho a la no discriminación como uno de los pilares básicos del Derecho de la Unión; la *Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO* (2021), también presta especial atención a los retos que plantean las decisiones algorítmicas porque pueden «reproducir y reforzar los sesgos existentes, lo que puede exacerbar las formas ya existentes de discriminación, los prejuicios y los estereotipos». Y el GT29 en sus *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 2018, subraya el peligro de que tanto la elaboración de perfiles como las decisiones automatizadas perpetúen los estereotipos existentes y la segregación social y lleven a discriminación injustificada (recuperado de

patrones históricos de discriminación contra las mujeres, ciertos grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, entre otros, es tenido en cuenta en el RIA para clasificar ciertos sistemas como de alto riesgo⁶. Tanto es así que en la Exposición de Motivos que contenía la Propuesta de RIA en su versión inicial, de 21 de abril de 2021, se declaraba expresamente que uno de los objetivos del establecimiento de requisitos específicos para los sistemas de alto riesgo era «*reducir al mínimo el riesgo de discriminación algorítmica, en particular en lo tocante al diseño y la calidad de los conjuntos de datos empleados para desarrollar sistemas de IA*», reconociendo con ello las principales causas que pueden provocarla⁷.

Previamente al RIA, las *Directrices éticas para una IA fiable del Grupo Independiente de Expertos de Alto Nivel sobre IA* de 2019 (en adelante, *Directrices éticas*) ya situaban la «*necesidad de evitar el sesgo algorítmico injusto*»⁸ entre los siete requisitos clave que debían cumplir los sistemas IA para ser considerados fiables. Tal como indica dicho documento, al que haremos especial referencia en este trabajo, la igualdad en el contexto de la IA implica la necesidad de evitar que el funcionamiento de este tipo de sistemas genere resultados injustamente sesgados, para lo que será preciso que los datos utilizados en su aprendizaje sean lo más inclusivos posibles de forma que estén representados los diferentes grupos de población⁹.

Asimismo, la doctrina ha identificado los ataques a la privacidad y la discriminación como amenazas especialmente significativas que derivan del uso de sistemas de IA para la toma de decisiones¹⁰. Reflejo de lo apuntado es que

<https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf>). Destacan esta idea también la *Carta de Derechos Digitales española* (2021) o la *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* (2023/C 23/01).

⁶ Vid., por ejemplo, los Considerandos 56 y 57. También en el Considerando 67 se reconoce expresamente que los sistemas de IA «*perpetúan y amplifican la discriminación existente, en particular con respecto a las personas vulnerables pertenecientes a determinados grupos, en particular grupos raciales o étnicos*».

⁷ Vid., ap.1.2.

⁸ Aunque «sesgo algorítmico» y «discriminación algorítmica» no son conceptos idénticos o coincidentes, en la práctica generalizada se emplean indistintamente para hacer referencia a las desviaciones de los sistemas de IA que conllevan resultados discriminatorios en forma de predicciones, recomendaciones o decisiones. Precizando las diferencias entre ambos conceptos, GERARDS, J./XENIDIS, *op.cit.*, p. 49.

⁹ Pp. 13 y 23. Disponible en: <https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>

¹⁰ Así se pone de manifiesto, por ejemplo, en EUBANKS, V., *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, St MARTÍN's Press, 2018; O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Capitán Swing, Madrid, 2017; GERARDS, J./ XENIDIS, R., *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law* (Special report European network of legal experts in gender equality and non-discrimination), European Commission, 2020; MANHEIM, K. M., & KAPLAN,

cada vez contamos con más evidencias de que las decisiones automatizadas no son siempre neutrales ni objetivas, sino que, muy al contrario, el riesgo de llegar a resultados parciales, sesgados o discriminatorios es más elevado de lo que, *a priori*, pudiera parecer. Algunos de los casos más mediáticos de discriminación algorítmica acaecieron hace ya algunos años en el seno de grandes empresas como Apple, Amazon o IBM, cuyos *softwares* demostraron tener prejuicios sexistas o racistas al haber sido entrenados con datos sesgados y tuvieron que ser retirados. Respecto de otros que también tuvieron una gran repercusión, contamos incluso con pronunciamientos judiciales que vienen marcando el rumbo a seguir en la materia. Así, el caso del algoritmo *Syri* (*Systeem Risico Indicatie*, o Sistema Indicativo del Riesgo) resuelto por el Tribunal de lo Civil de la Haya en su sentencia de 5 de febrero de 2020; el caso del algoritmo *Frank*, resuelto por el Tribunal Ordinario de Bolonia en sentencia de 31 de diciembre de 2020; o el caso *Loomis v. Wisconsin*, conocido por el Tribunal Supremo de Wisconsin (EEUU), que giró en torno a un sistema inteligente de evaluación de riesgos denominado *COMPAS* (*Correctional Offender Management Profiling for Alternative Sanctions*). En todos ellos se evidenció que el algoritmo (o el uso que se hacía del sistema) discriminaba a ciertos colectivos¹¹.

L., «Artificial Intelligence: Risks to Privacy and Democracy», *Yale Journal of Law and Technology* 106, vol. 21, 2019, pp. 106-189, disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016; GINÉS i FABRELLAS, A., «Sesgos discriminatorios en la automatización de decisiones en el ámbito laboral: evidencias de la práctica», en RIVAS VALLEJO, P. (dir.), *Discriminación algorítmica en el ámbito laboral*, 2022; o los trabajos de SORIANO ARNANZ, A. «Decisiones automatizadas y discriminación: aproximación y propuestas generales», *Revista General de Derecho Administrativo*, N°. 56, 2021, «Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos», *Revista de Derecho Público: teoría y método*, N°13, 2021, pp. 85-127, y «La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial», en *Nuevas normatividades: inteligencia artificial, derecho y género* (coord. por P.R. Bonorino Ramírez / R. Fernández Acevedo / P. Valcárcel Fernández), Navarra, 2022, pp. 63-88; MUÑOZ GUTIÉRREZ, C., «La discriminación en una sociedad automatizada: Contribuciones desde América Latina», *Revista chilena de derecho y tecnología*, 10(1), 2021, p. 273; SÁNCHEZ CAPARRÓS, M. «Prevenir y controlar la discriminación algorítmica», 2022. Recuperado de https://www.researchgate.net/publication/358207305_Prevenir_y_controlar_la_discriminacion_algoritmica, p. 17/34; o GASCÓN MARCÉN, A., «Derechos humanos e inteligencia artificial», en *Setenta años de Constitución Italiana y cuarenta años de Constitución Española*, Pérez Miras (dir.), Teruel Lozano (dir.), Raffiotta (dir.), Pia Iadicco (dir.), Vol. 5, 2020 (Retos en el siglo XXI / coord. por Silvia Romboli), p. 337.

¹¹ Otros ejemplos que demuestran que en la práctica estos casos son más frecuentes de lo que sería deseable, los protagonizaron Google o Microsoft. En el primer caso, cuando el algoritmo de clasificación de *Google Photos* después de su aprendizaje automático confundió a varios jóvenes afroamericanos con gorilas o cuando se demostró que su algoritmo publicitario mostraba ofertas de empleo mejor remuneradas a los hombres que a las mujeres. En caso de Microsoft, cuando el *chatbot Tay*—que se servía de la IA para mantener conversaciones en una conocida red social con un público de entre 18 y 24 años—, empezó a elaborar mensajes de contenido racista, sexista y xenófobo, y tuvo que ser retirado por la compañía al día siguiente de su lanzamiento. También en el sector de la conducción autónoma se ha observado el sesgo racial, al demostrar un estudio llevado a cabo por investigadores del Instituto Tecnológico de Georgia (EEUU) sobre ocho sistemas de inteligencia artificial emplea-

Sin duda, el empleo de sistemas de IA para la toma de decisiones ha hecho que la discriminación adquiriera unas dimensiones y afronte unos retos hasta el momento inexistentes¹². De hecho, los expertos vienen advirtiendo desde hace años sobre la potencialidad de la tecnología para *extraer y procesar datos*, pero también para *reproducir y perpetuar discriminaciones existentes, amplificar sesgos* y, lo que es aún más peligroso, para *hacer que la discriminación pase desapercibida*¹³. De ahí que se haya mantenido, con acierto a nuestro juicio, que uno de los rasgos definitorios y más problemáticos de la discriminación algorítmica es precisamente su *invisibilidad*, junto con su intensidad y su complejidad técnica¹⁴. Dichas características y sus consiguientes desafíos, justifican que se haya convertido en un fenómeno nuevo y distinto que obliga a hacer ajustes en los mecanismos de tutela antidiscriminatoria existentes incorporando exigencias de transparencia y explicabilidad desde el diseño, evaluaciones de impacto que midan el potencial de discriminación del sistema por diversas causas (género, etnia, religión etc.) y auditorías, con el fin de poder detectar

dos en la detección de objetos, que tendían a favorecer los tonos claros de piel sobre los oscuros y discriminaban a los peatones en función de dicho rasgo. Y en otro estudio realizado respecto de un algoritmo utilizado por aseguradoras y hospitales en EEUU para analizar los riesgos de salud de los pacientes y asignar atención médica, también se advirtió que el sistema discriminaba sistemáticamente a la población afroamericana.

¹² En este sentido, por todos, GINÈS i FABRELLAS, A., *op.cit.*, pp. 316 y ss. También GERARDS, J./ XENIDIS, R., *op.cit.*, p. 75, ponen de manifiesto que, si bien muchos de los problemas que plantea la discriminación existían antes del desarrollo de los algoritmos y han sido identificados por la doctrina, el uso creciente de algoritmos en todos los ámbitos de la sociedad los agudiza y multiplica.

¹³ Estos peligros han sido puestos de manifiesto por la mayoría de la doctrina que ha tratado el tema. Pueden verse, entre otros, los trabajos citados *supra* en nota 10. Con detalle explica cada uno de ellos, GINÈS i FABRELLAS, A., *op.cit.*, pp. 315-321. También ALAMEDA CASTILLO, M.T., «Reclutamiento tecnológico. Sobre algoritmos y acceso al empleo», *Temas laborales: Revista andaluza de trabajo y bienestar social*, N° 159, 2021, p. 14. Ya en el año 2017, el Parlamento Europeo alertaba en su *Resolución de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica* (2015/2103(INL)) de que el aprendizaje automático ofrecía enormes ventajas económicas a la sociedad al mejorar enormemente la capacidad de analizar datos, pero también planteaba retos a la hora de velar por la no discriminación, las garantías procesales, la transparencia y la inteligibilidad de los procesos decisorios. Vid., Considerando letra h). También en el apartado sobre Principios éticos señala que «el potencial de empoderamiento que encierra el recurso a la robótica se ve matizado por una serie de tensiones o posibles riesgos y que debe ser evaluado detenidamente a la luz de la seguridad y la salud humanas; la libertad, la intimidad, la integridad y la dignidad; la autodeterminación y la no discriminación, y la protección de los datos personales» (n° 10).

¹⁴ Así lo mantienen, entre otros, SÁEZ LARA, C., «El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación», *Temas laborales: Revista andaluza de trabajo y bienestar social*, N° 155, 2020, p. 45, para quien este rasgo es, a su vez, el principal problema de estas tecnologías; ALAMEDA CASTILLO, M.T., *op.cit.* p. 14, siguiendo a la primera; o EGUÍLUZ CASTAÑEIRA, J.A., «Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales», *Estudios de Deusto: revista de Derecho Público*, vol. 68, n. 2, 2020, p. 337.

la discriminación, prevenirla o corregirla y, en última instancia, reparar los daños que ocasione¹⁵.

Precisamente a las medidas dirigidas a garantizar la transparencia y explicabilidad de los sistemas de IA para detectar y prevenir errores, sesgos y discriminación injusta dedicaremos el presente trabajo, que comenzará abordando la opacidad algorítmica en sus diversas manifestaciones como principal obstáculo para la consecución de dichos objetivos. Tras ello, se analizará qué significa concretamente que los sistemas de IA deban ser transparentes y explicables y qué soluciones se han venido adoptando para conseguirlo, dedicando particular atención a las previstas en el RGPD y en el RIA.

2. LA OPACIDAD COMO PRINCIPAL ESCOLLO PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA

2.1. CONSIDERACIONES PREVIAS

Los principales desafíos que plantean los sistemas de IA tanto para la salud, la seguridad y los derechos fundamentales en general, como para la igualdad y no discriminación en particular, están directamente relacionados con sus características intrínsecas. Su complejidad técnica, interconectividad, opacidad, vulnerabilidad, apertura, autonomía y capacidad de autoaprendizaje, así como la pluralidad de agentes involucrados en su diseño, desarrollo, implementación y uso, dificultan la averiguación de *cuándo, cómo o por qué* se ha originado el error del sistema y *quién debe responder* de los daños que se ocasionen¹⁶.

¹⁵ Para MERCADER UGUINA, J.R., *op.cit.*, p. 6, aunque por el momento la discriminación algorítmica obtiene respuestas desde nuestras actuales técnicas conceptuales, requiere que se adopten nuevas herramientas jurídicas de análisis.

¹⁶ El Grupo de Expertos en responsabilidad civil y nuevas tecnologías (*Expert Group on Liability and New Technologies - New Technologies Formation*, conocido por sus siglas en inglés NTF), en su Informe titulado *Liability for artificial intelligence and other emerging digital technologies*, de 21 de noviembre de 2019, explicaba una serie de características comunes a las tecnologías digitales emergentes en general que podían complicar la determinación de la responsabilidad civil cuando se ocasionaran daños. Dichas características eran las siguientes: (a) complejidad, (b) opacidad, (c) apertura, (d) autonomía, (e) previsibilidad, (f) manejo y dependencia de datos, y (g) vulnerabilidad. Estas características también se recogen por la Comisión Europea en su *Informe al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020* (COM/2020/64 final). Explica cada uno de estos rasgos, por todos, ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, 2022, pp. 56-66.

A nuestro modo de ver, de todas estas características es la *opacidad* la que se sitúa en el origen de la mayoría de los problemas mencionados, ya que, la falta de transparencia tanto a la hora de *utilizar* estos sistemas para tomar decisiones que afectan a personas concretas, como a la hora de *explicar los motivos* que las sustentan, hace que sea extraordinariamente difícil para el ciudadano averiguar y demostrar que está siendo discriminado¹⁷.

Ya advertía el Parlamento Europeo en su *Resolución de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL))¹⁸, que la opacidad algorítmica podía hacer extremadamente costoso, o incluso imposible, determinar *quién controlaba el riesgo asociado al sistema de IA, o qué código, entrada o datos provocaban en última instancia el funcionamiento lesivo, o la identificación de la relación de causalidad entre el daño y el comportamiento que lo causa*, con el resultado de que las víctimas podían quedar sin recibir una indemnización adecuada. Y la misma idea la reitera la Comisión a lo largo de su última *Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial*, de 28 de septiembre de 2022 (COM/2022/496 final)¹⁹.

Para LAZCOZ MORATINOS la opacidad es la «preocupación que más atención ha despertado en la literatura al evaluar la aplicación de estos modelos algorítmicos en la toma de decisiones»²⁰. Es por ello que, como se irá viendo a lo largo de estas páginas, en todos los instrumentos normativos vigentes o proyectados relacionados con la IA, tanto en el ámbito europeo como fuera de él, la transparencia se erige en pieza clave o principio rector a la hora de diseñar, desarrollar e implementar algoritmos para la toma de decisiones. De

¹⁷ En el estudio realizado por GERARDS, J./ XENIDIS, R., *op.cit.*, p. 108, se destaca que los problemas de discriminación de los sistemas de IA pueden ser difíciles de detectar y confrontar debido principalmente a problemas de transparencia y responsabilidad.

¹⁸ Vid., Considerando H).

¹⁹ Vid., por ejemplo, pp. 1, 16 y Considerandos 3 o 27. En el Considerando 3 señala que «cuando la IA se interpone entre el acto u omisión de una persona y el daño, las características específicas de determinados sistemas de IA, como la opacidad, el comportamiento autónomo y la complejidad, pueden hacer excesivamente difícil, si no imposible, que el perjudicado satisfaga la carga de la prueba. En particular, puede resultar excesivamente difícil demostrar que un dato de entrada concreto del que es responsable la persona potencialmente responsable ha dado lugar a una información de salida específica de un sistema de IA que, a su vez, ha provocado el daño en cuestión».

²⁰ Así lo afirma LAZCOZ MORATINOS, G., «Análisis jurídico de la toma de decisiones algorítmica en la asistencia sanitaria», en *La regulación de los algoritmos*, coord. por G.M. Díaz González/A.J. Huergo Lora (dir.), 2020, p. 286. También TOLOSA, P./DIBO, C., «Inteligencia artificial, discriminación por género y Derecho: viejos problemas, nuevos desafíos», en C. Danesi (dir.) *Inteligencia Artificial, tecnologías emergentes y Derecho*, 2021, p.187, consideran que los algoritmos deben ser auditables, transparentes, y explicables y si se logra implementar algoritmos con tales características seguramente las decisiones que se obtengan podrán ser más transparentes que las decisiones humanas bien intencionadas, pero inconscientemente sesgadas.

hecho, en las Directrices éticas del Grupo de Expertos en IA se incluye como uno de los siete requisitos esenciales a cumplir por los sistemas para conseguir una IA fiable. Y en la *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))* –en adelante, Resolución PE sobre aspectos éticos de la IA 2020–, se estableció que el marco regulador de la IA debía regirse por los principios de transparencia, explicabilidad, equidad, rendición de cuentas y responsabilidad, con el fin de potenciar las ventajas de los sistemas y proteger al mismo tiempo a los ciudadanos de los riesgos que implican. Dicha protección, tal como subraya el Parlamento, implica que los humanos puedan comprender las acciones de la IA, para lo cual es imprescindible que los desarrolladores e implementadores garanticen, dentro de los límites de lo técnicamente posible, que la tecnología se despliega y utiliza respetando los requisitos de transparencia y permitiendo la auditoría y la trazabilidad.

2.2. OPACIDAD EN EL USO Y SOBRE EL CONTENIDO DE LOS ALGORITMOS

Conviene precisar, de entrada, que la opacidad algorítmica puede y suele manifestarse tanto a la hora de revelar que se están usando estos sistemas para decidir cuestiones concretas, como a la hora de proporcionar información sobre ellos que permita a los interesados saber cómo y en base a qué motivos se ha adoptado la decisión que les afecta. Es decir, en muchas ocasiones las personas ignoramos que estamos siendo objeto de decisiones algorítmicas y de que, por ejemplo, las mismas nos discriminan injustamente. Así, una persona que ha sido discriminada por una plataforma de Internet en relación con el precio de determinados productos en función de su perfil (incluido su género, edad, etc.) puede que ni siquiera sepa que la oferta que se le muestra ha sido decidida por un sistema inteligente y menos aún que el mismo puede estar vulnerando sus derechos, sobre todo cuando no tiene una referencia comparativa, es decir, si no sabe que a otras personas que cuentan con atributos diferentes se le ofrecen los mismos productos a un mejor precio²¹.

El Parlamento Europeo, en su *Resolución sobre aspectos éticos de la IA 2020*, hacía una sutil referencia a esta idea al distinguir entre la *transparencia de*

²¹ Expone esta situación SORIANO ARNANZ, A. «Decisiones automatizadas y discriminación: aproximación y propuestas generales», *Revista General de Derecho Administrativo*, N.º. 56, 2021, p. 17/31, para quien, el acceso a la justicia para defender el derecho a la igualdad de trato y no discriminación no sólo se ve condicionado por cuestiones económicas o burocráticas, sino también por el hecho de que las víctimas de las situaciones de discriminación con frecuencia no son conscientes de que sus derechos están siendo vulnerados.

los algoritmos y la transparencia en el uso de los algoritmos²². Y también en su Resolución de 12 de febrero de 2020, sobre los procesos automatizados de toma de decisiones: garantizar la protección de los consumidores y la libre circulación de bienes y servicios (2019/2915 (RSP)), advertía de que el uso de procesos automatizados de toma de decisiones planteaba retos para los consumidores que podían afectar tanto a su capacidad para detectar dichos procesos, como de entender su funcionamiento, tomar decisiones con conocimiento de causa en cuanto a su utilización y autoexcluirse²³.

En virtud de lo anterior, consideramos junto a un sector de nuestra doctrina que habría que distinguir dos niveles de opacidad algorítmica²⁴. El primero sería aquel en que el interesado desconoce que es objeto de una decisión automatizada, y el segundo, aquel en que sabe que la decisión que le afecta ha sido o va a ser adoptada por un sistema de IA pero no se le permite conocer el funcionamiento del proceso decisorio ni los motivos de la decisión que le afecta negativamente.

Como es lógico, si ni siquiera sabemos que estamos siendo objeto de decisiones algorítmicas, menos aún seremos capaces de descubrir que las mismas son discriminatorias y, en consecuencia, perderemos la oportunidad de impugnarlas en defensa de nuestros derechos²⁵. De lo que no cabe duda es de que, en tales casos, la frustración de las legítimas expectativas de las personas o la pérdida de oportunidad de acceder a un empleo, conseguir un crédito, ingresar en un prestigioso centro educativo o ser beneficiario de un tratamiento médico o de un seguro de vida (entre otros muchos ejemplos que podrían ponerse) basadas en criterios injustos o discriminatorios, generan daños a personas concretas que en muchos casos quedarán sin resarcir por desconocimiento o ignorancia acerca de que, tras esas decisiones, se esconde un proceso algorítmico y de que el mismo arroja resultados discriminatorios.

²² Vid., ap. 20.

²³ Vid., ap. C).

²⁴ LAZCOZ MORATINOS, G., *op.cit.*, p. 293, VESTRI, G., «La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativ», *Revista Aragonesa de Administración Pública*, n° 56, 2021, p. 382.

²⁵ En la misma línea considera LLORENS ESPADA, J., «Responsabilidades civiles por discriminación por razón de género cuando medie un sistema de inteligencia artificial», en Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, p. 576, que en el ámbito laboral será difícil para un trabajador saber si una decisión empresarial esconde un proceso algorítmico, o incluso sabiéndolo, no será fácil obtener información de los motivos en base a los cuales el algoritmo toma las decisiones y de qué parte del proceso deriva la falta de equidad. Por ende, el trabajador no podrá saber que está siendo discriminado ni podrá incoar un procedimiento de tutela de sus derechos fundamentales ante casos de discriminación generados por algoritmos. En sentido parecido, EGUÍLUZ CASTAÑEIRA, J.U., *op.cit.*, p. 337.

Es más, aun siendo conscientes de que detrás de la decisión que nos afecta se esconde un proceso algorítmico, seguiría siendo muy difícil *detectar* posibles errores o casos específicos de discriminación teniendo en cuenta que la decisión algorítmica se basa en una combinación de múltiples variables con ponderaciones diversas a las que el ciudadano en principio no tiene acceso o, incluso teniéndolo, no comprende. Y es que en muchas ocasiones estos sistemas de IA son técnicamente tan complejos que ni siquiera los programadores pueden explicar las razones por las que ha llegado a una decisión y no a otra distinta.

Urge por tanto, como paso previo, que la ciudadanía tome plena conciencia de que hoy en día muchas de las decisiones que nos afectan -y que normalmente se basan en nuestros datos personales- están siendo *adoptadas por algoritmos o en base a ellos*, que pueden contener sesgos y arrojar resultados que vulneran nuestro derecho a la igualdad de trato y a la no discriminación. Sólo así se podrá superar el primer escollo que presenta la discriminación algorítmica que no es otro que su detección o identificación.

2.3. OPACIDAD JURÍDICA Y TÉCNICA DEL ALGORITMO

Asimismo, en el tratamiento del problema de la opacidad algorítmica inciden factores tanto técnicos como jurídicos. Es decir, la falta de transparencia puede deberse tanto a la propia complejidad intrínseca del algoritmo, cuya comprensión exige una capacidad analítica y unos conocimientos técnicos considerables, como al régimen jurídico que lo protege en tanto en cuanto pueda ser objeto de derechos de propiedad intelectual o secreto empresarial²⁶. Esta doble opacidad, que dificulta tanto el *acceso* como la *comprensión*

²⁶ La doctrina ha hecho referencia a esta idea de varias maneras. Por ejemplo, para LAZCOZ MORATINOS, G., *op.cit.*, p. 293, en el ámbito de la IA la opacidad es polisémica y puede utilizarse con un doble sentido: por un lado, como equivalente a *ininteligible* (inherente al *machine learning in a big data context*), y por otro lado, para designar la opacidad intencionada en base a razones de derechos de autor, secreto industrial, privacidad o seguridad. Para SUBERBIOLA GARBIZU, I., «Inteligencia artificial, opacidad y motivación de las decisiones administrativas automatizadas», en *La protección de los derechos fundamentales en el ámbito tributario*, coord. por A.Vázquez del Rey Villanueva e I. Suberbiola Garbizu, 2021, recuperado de La Ley Digital (LA LEY 1117/2021), hay que ser conscientes de que existen *black boxes* por la arquitectura del propio sistema de IA y *black boxes* inducidas por la normativa que lo regula. Y CASTILLO OCARANZA, C., «Discriminación algorítmica en el ámbito laboral», en P. Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, p. 75, considera que la opacidad algorítmica podría ser incluso triple, ya que, junto a la opacidad legal y a la opacidad técnica debida a la complejidad inherente al propio sistema, habría que añadir la inducida a través de «mecanismos de ofuscación intencional» utilizados para alterar las instrucciones de un programa (esto es, su código fuente) de forma que, a pesar de seguir manteniendo su función original, se hicieran difíciles de leer.

del sistema, pone en tela juicio el derecho a obtener una resolución o decisión motivada y la posibilidad de recurrirla, generando indefensión para el afectado y un grave riesgo de arbitrariedad, sobre todo cuando estos sistemas son utilizados por la Administración puesto que en el ámbito público las exigencias de transparencia en los procesos decisorios se acrecientan.

Respecto a la opacidad técnica o consustancial al algoritmo, la misma aumenta cuando se emplean algoritmos de autoaprendizaje no supervisado y profundo que gozan de gran autonomía decisoria y cuya capacidad predictiva (altamente precisa por otro lado) reside en establecer correlaciones tan sumamente complejas que sus resultados pueden ser ininteligibles para el ser humano a partir de los datos que se aportan al modelo²⁷. Este efecto, conocido como «caja negra» o *black box*, hace referencia a la imposibilidad de identificar las razones que han llevado al sistema de IA a adoptar sus decisiones. Por ello, el uso de esta tecnología plantea un problema estructural en la medida en que su esencia misma choca con las normas que exigen transparencia, trazabilidad y posibilidad de identificar los procesos de toma de decisiones de los algoritmos.

Respecto a este tipo de sistemas donde la lógica computacional es elusiva y opaca, ni siquiera la apertura de la caja negra y el acceso al código fuente del algoritmo garantizaría la comprensibilidad o inteligibilidad de los resultados²⁸. Este problema estructural hace que la propia idea de la transparencia resulte cuestionable e incluso se hable de la «falacia de la transparencia»²⁹,

²⁷ Apunta BARRIOS ANDRÉS, M., *Manual de Derecho Digital*, Valencia, 2020, p. 62, que el término «profundo» hace referencia al gran número de capas de neuronas ocultas en la red. A diferencia del aprendizaje automático supervisado, en el que han de realizarse manualmente los procesos iniciales de extracción de características relevantes y diseño de un modelo capaz de categorizar o clasificar la información que se desea analizar, en los de aprendizaje profundo estos procesos de extracción de características y modelización son automáticos. Los hace el sistema a partir de imágenes, textos o sonidos. Son altamente precisos y en ocasiones superan el rendimiento humano.

²⁸ Así lo afirman, entre otros muchos, SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal: los sistemas algorítmicos de evaluación de riesgos», en *Dimensiones éticas y jurídicas de la inteligencia artificial en el marco del Estado de Derecho*, J.I. Solar Cayón (ed.), Alcalá de Henares, 2020, p. 149; RIVAS VALLEJO, P. «Análisis desde el derecho antidiscriminatorio», en P. Rivas Vallejo (dir.) *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, p. 441 EVANGELIO LLORCA, R., «Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por N. Álvarez Lata; J.M. Busto Lago (pr.), 2024, p. 561. No obstante, como mantiene NAVAS NAVARRO, S., «Sistemas expertos basados en inteligencia artificial y responsabilidad civil. Algunas cuestiones controvertidas», *Diario La Ley*, 13 de Diciembre de 2019, LA LEY 14980/2019, p. 7/16, si bien el acceso a la *black box* no será la panacea para la víctima, quizá sí que sea de utilidad para fijar indicios.

²⁹ SOLAR CAYÓN, J.I., *op.cit.*, p. 148. También advierte el NIST (*National Institute of Standards and Technology*) que la transparencia no garantiza la explicabilidad, especialmente si el usuario no comprende los principios técnicos. Vid., *AI Risk Management Framework: Initial Draft*, 17 de marzo

ya que no siempre que se consigue acceder a la caja negra de los sistemas algorítmicos quedan salvaguardados adecuadamente los derechos de los interesados. Especialmente a los efectos de la asignación de responsabilidad, el acceso a la información de las cajas negras puede no ser suficiente para lograr una conexión entre el autor, el algoritmo y sus consecuencias, que sea lo suficientemente sustancial como para que alguien pueda considerarse responsable de sus efectos perjudiciales³⁰. Pero es que, además, incluso cuando se pudiera detectar la causa del problema, la misma podría variar o desaparecer con el tiempo teniendo en cuenta que este tipo de algoritmo está en constante evolución³¹.

Por estos motivos, un sector doctrinal considera que, aun a costa de sacrificar sus ventajas (principalmente, su mayor nivel de precisión), debe demostrarse el empleo de este tipo de sistemas de aprendizaje profundo en los que no se puede garantizar el respeto de los derechos fundamentales³². De hecho,

de 2022. Accesible en <https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf>

³⁰ GONZÁLEZ VALVERDE, A., «Responsabilidad por el potencial de sesgo discriminatorio de los algoritmos de los productos de Inteligencia Artificial. A propósito de la Algorithmic Accountability Act of 2019 (s.1108)». En Ataz López y Cobacho Gómez, *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillaumon*, Vol. 2, 2021, pp. 1263-1264. Las instituciones europeas han venido advirtiendo de este *handicap* en diferentes documentos, destacando que dicho efecto de caja negra podría llegar a impedir que los afectados obtuvieran una indemnización por los daños causados por aplicaciones de IA autónomas. Vid., por ejemplo, el *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la IA, el internet de las cosas y la robótica*, de 19 de febrero de 2020, de la Comisión.

³¹ Precisamente por ello se venía abogando por la necesidad de que esta tecnología contara con un sistema que permitiera registrar información sobre su funcionamiento, esto es, datos relativos a su movimiento, actuación y decisión («logging by design» o registro desde el diseño) a modo de *caja negra* como la que se encuentra hoy en día en aviones, trenes o drones. Entre otros lo defendían, NAVAS NAVARRO, S., «La perspectiva de género en la inteligencia artificial», *Diario La Ley*, n° 48, Sección Ciberderecho, 8 de marzo de 2021, pp. 8 y 11/23, basándose en el Informe del *Expert Group on Liability and New Technologies, Liability*, o SORIANO ARNANZ, A., «La aplicación del marco jurídico europeo...», *cit.*, p. 81, para quien en los sistemas que se van actualizando, es necesario que los operadores guarden una copia de cada versión del programa utilizado en los procesos de toma de decisiones.

³² En el ámbito europeo, el Informe *AI in the UK: ready, willing and able?*, elaborado por el Comité sobre inteligencia artificial de la Cámara de los Lores británica, recomienda que el empleo de sistemas de IA basados en redes neuronales profundas que puedan tener un impacto sustancial en la vida de los individuos se demore hasta que se encuentren soluciones técnicas que permitan su comprensibilidad plena (párrafo 105). Accesible en: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm>. En relación con esto, considera ALCOLEA AZCÁRRAGA, C., «La responsabilidad patrimonial de la Administración y el uso de algoritmos», *Revista General de Derecho Administrativo*, n° 59, enero 2022, p.8/31, la posibilidad de extrapolar al ámbito tecnológico el *principio de precaución* aplicable en Derecho ambiental. Con el fin de controlar las consecuencias imprevisibles de los sistemas de IA y evitar daños irreparables, esgrime que podría adoptarse el principio de precaución algorítmica, por cuanto el ámbito tecnológico tiene también un importante potencial dañino para la humanidad en su conjunto. En base a dicho principio de precaución concluye

la ininteligibilidad de algunos algoritmos de caja negra ha frenado su empleo en sectores como la medicina, limitando su uso como soporte o apoyo en la toma de decisiones clínicas³³. No obstante, frente a esta cautelosa postura, la opinión mayoritaria aboga por la utilización de tales sistemas adoptando, eso sí, un enfoque de «explicabilidad» sobre la mera transparencia técnica, conceptos ambos que se analizarán el siguiente apartado³⁴. Tanto es así, que existe actualmente una tendencia a desarrollar modelos algorítmicos más sencillos, transparentes y explicables que respondan mejor a las exigencias jurídicas y generen mayor confianza en los usuarios, que ha dado lugar a un campo de estudio e investigación denominado *Explainable Artificial Intelligence* o *Interpretable Machine Learning*, a través del que se pretende encontrar un equilibrio adecuado entre la optimización de la capacidad predictiva de los algoritmos y su explicabilidad³⁵. De lo que se trataría, en definitiva, sería de integrar la transparencia como estrategia *ex ante* y la explicabilidad *ex post*, para que los usuarios de estos sistemas de IA pudieran comprender el porqué de sus decisiones y rebatirlas si lo desean.

Junto con esta opacidad estructural del algoritmo, nos encontramos con la opacidad jurídica en la medida en que el acceso al mismo (tanto a su código fuente como a los datos utilizados por el sistema de IA para funcionar y aprender) podría denegarse al interesado si se considera protegido por derechos de propiedad intelectual o como secreto empresarial³⁶.

el autor que, aunque algunos «autores consideran que la aplicación de los algoritmos a las facultades discrecionales de la Administración pública aportaría un baremo nuevo que alejaría la arbitrariedad, podría parecer que su uso sin una completa comprensión de cómo funcionan o por qué toman las decisiones que toman debería postergarse a un momento en que efectivamente se disponga de ese control y posibilidad de fiscalización». Recuperado de <https://laadministracionaldia.inap.es/noticia.asp?id=1512629>.

³³ LAZCOZ MORATINOS, G., *op.cit.*, p. 293.

³⁴ COTINO HUESO, L., «Transparencia de la inteligencia artificial pública...», *cit.*, señala, citando a Gutiérrez David, que la «transparencia técnica sería una característica pasiva del modelo de IA que permite al observador humano comprender o entender el sistema, mientras que habría otros sistemas de IA que no son transparentes, pero pueden llegar a ser explicables mediante distintas técnicas a partir del comportamiento del modelo, los datos utilizados, los resultados obtenidos y del proceso completo de la toma de decisión».

³⁵ Esta necesidad de encontrar un equilibrio entre la mejora de la explicabilidad de un sistema (que puede reducir su precisión) o una mayor precisión del mismo (a costa de la explicabilidad), ya se ponía de relieve en las *Directrices éticas* del Grupo de Expertos. En dicho documento se establecía la necesidad de que cuando un sistema de IA tuviera un impacto significativo en la vida de las personas, debería ser posible reclamar una explicación adecuada del proceso de toma de decisiones del sistema de IA (*vid.*, ap. 77).

³⁶ Se ha mantenido que los algoritmos podrían quedar protegidos por la *Ley 1/2019, de 20 de febrero de 2019, de secretos empresariales*, siempre que reunieran las condiciones necesarias para ser considerados como secreto empresarial, esto es, siempre que se tratase de información no divulgada por las empresas, que tuviera valor comercial y se hubieran adoptado medidas razonables para su protección. En este sentido, por ejemplo, la STS n. 508/2018, de 20 de septiembre, confirmó que

Asimismo, se han esgrimido razones de seguridad pública para no ofrecer información sobre los algoritmos utilizados por la Administración, impidiendo a los particulares afectados conocer el proceso decisorio y las razones por las que se ha llegado al resultado que les perjudica.

Así ocurrió, por ejemplo, en el polémico caso del algoritmo *Bosco* para la concesión del bono social eléctrico a personas vulnerables³⁷. Ante las abundantes quejas de usuarios a los que se les había denegado la ayuda y creían tener derecho ella, la Fundación CIVIO solicitó a la Administración, al amparo de la Ley de Transparencia, que le proporcionara su especificación técnica, los resultados de las pruebas de comprobación de la aplicación y su código fuente, a fin de comprobar si el programa presentaba algún defecto o errores en su configuración que impedían la correcta aplicación de la legislación³⁸.

el código fuente de un programa informático podía estar protegido como secreto comercial si su divulgación suponía un perjuicio económico para su titular y siempre que se hubiera mantenido en secreto. Mayor polémica ha generado su protección por los derechos de autor regulados en el título VII LPI. Aunque no podemos profundizar ahora en este asunto, simplemente mencionaremos que hay quien defiende que la definición de «programa de ordenador» del art. 96.1 LPI es aplicable al algoritmo en tanto que secuencia de instrucciones que constituyen el motor de funcionamiento de cualquier programa informático y por ende quedaría protegido por los derechos de autor, y para otro sector doctrinal no estaría protegido por esta vía en tanto en cuanto la *Directiva 2009/24/CE sobre la protección jurídica de los programas de ordenador*, en su Considerando 11, aclara que solo se protege la expresión del programa de ordenador pero no *las ideas y principios implícitos en los elementos del programa, incluidas las de sus interfaces*, disposición que después se recoge en su art. 1.2 y que también establece el art. 96.4 LPI. En este último sentido, ALAMEDA CASTILLO, M.T., *op.cit.* p. 34 o CASTILLO PARRILLA, J.A., «Sentencia del Tribunal Ordinario de Bolonia de 31 de diciembre de 2020 (Caso Deliveroo) ¿Discriminación algorítmica o discriminación a través de un algoritmo?», *Derecho Digital e Innovación. Digital Law and Innovation Review*, n.7 (octubre-diciembre), 2020, para quien la protección jurídica de los algoritmos se reduce a su protección como secretos comerciales, ya que no pueden ser objeto de derechos de autor ni son patentables. Defendiendo la primera postura, RIVAS VALLEJO, P. «Análisis...», *cit.*, p. 442, citando también la sentencia del TJUE de 22 de diciembre de 2010 (asunto *Bezpečnostní softwarová asociace*), favorable a la protección del algoritmo en base a la Directiva 2009/24/CE.

³⁷ Se trata de un *software*, de titularidad pública pero gestionado por empresas privadas, que determina qué consumidores en situación de vulnerabilidad tienen derecho a un descuento en la factura de la luz. La concesión de este beneficio no es una decisión discrecional de la Administración, sino que las condiciones para obtenerlo y la forma de solicitarlo están previstas en la ley. Se regula en el Real Decreto 897/2017 (desarrollado por la Orden ETU/943/2017) que aplica una tarifa eléctrica reducida a consumidores vulnerables. Sobre este caso, puede verse, entre otros, BAZ LOMBA, C. (2021). Los algoritmos y la toma de decisiones administrativas. Especial referencia a la transparencia. *Revista CEFLegal*, 243, 119-160; también COTINO HUESO, L., «Caso Bosco, a la tercera tampoco va la vencida. Mal camino en el acceso los algoritmos públicos», *Diario LA LEY*, N° 84, Sección Ciberderecho, 17 de Mayo de 2024.

³⁸ En principio, la aplicación debía ser neutral porque solo tenía que realizar la mera aplicación de los requisitos de acceso a la prestación sin cambiar nada del panorama legal ni práctico. Sin embargo, tras su implantación, la mitad de los anteriores beneficiarios dejaron de ser idóneos para el reconocimiento del bono social. De aquí se infiere que, aunque en principio las reglas del juego sean idénticas, la forma de trabajar de los algoritmos que eleva exponencialmente el índice de gra-

Tanto el Ministerio para la Transición Ecológica, como el CTBG y los diferentes órganos judiciales que conocieron el asunto, denegaron a CIVIO el acceso al código fuente basándose en que afectaría no sólo a los derechos de propiedad intelectual sobre el *software*, sino también a la seguridad pública y a la defensa nacional por la conexión del sistema con bases de datos de carácter sensible cuya integridad podía verse comprometida³⁹. La Sala de lo Contencioso-Administrativo de la Audiencia Nacional (sección séptima), en su reciente sentencia de 30 de abril de 2024 (que rechaza por tercera vez la petición de acceso al código fuente), reitera que el mismo está protegido por la Ley de Propiedad Intelectual y que carece de todo fundamento excluir a la Administración del derecho de la protección intelectual. Además, considera que la difusión del código fuente de la aplicación *Bosco* pondría en grave riesgo derechos de terceros y atentaría a bienes jurídicos protegidos por los límites al derecho de acceso a la información pública del artículo 14.1 letras d), g), i) y k). Concluye que, sin lugar a dudas, la ocultación del código fuente de la aplicación es garantía de protección ante las vulnerabilidades⁴⁰.

Aunque éste no es el único caso sobre decisiones algorítmicas que ha sido objeto de resolución judicial por nuestros tribunales y órganos administrati-

nularidad del análisis de datos disponibles, cambia los resultados. Así lo explica RIVAS VALLEJO, P., «Sesgos de automatización y discriminación algorítmica», en *Discriminación algorítmica en el ámbito laboral*, Pilar Rivas Vallejo (dir.), 2022, pp. 52-53.

³⁹ Nos parecen interesantes las consideraciones que realiza el CTBG sobre la protección jurídica del código fuente: «El código fuente es el archivo o conjunto de archivos que tienen un conjunto de instrucciones muy precisas, basadas en un lenguaje de programación, que se utiliza para poder compilar los diferentes programas informáticos que lo utilizan y se puedan ejecutar sin mayores problemas [...]. El *software* ha sido extraordinariamente difícil de clasificar como materia específica de propiedad intelectual debido a que su doble naturaleza plantea problemas particulares para quienes tratan de establecer analogías con las categorías jurídicas existentes. Esta es la razón por la que ha habido intentos de clasificarlo como objeto de derechos de autor, de patentes o de secretos comerciales, e incluso como un derecho *sui generis* de *software* [...] Éste es el enfoque vigente respecto de la protección del software en diversos tratados internacionales. Así, por ejemplo, el artículo 4 del Tratado de la OMPI sobre Derecho de Autor (WCT), el artículo 10 del Acuerdo sobre los ADPIC de la Organización Mundial del Comercio y el artículo 1 de la Directiva (91/250/CEE) del Consejo Europeo sobre la protección jurídica de programas de ordenador equiparan el software con las obras literarias, protegidas por el derecho de autor. A efectos de la Directiva, el término «programa de ordenador» incluye programas en cualquier forma, incluso los que están incorporados en el «hardware»; este término designa también el trabajo preparatorio de concepción que conduce al desarrollo de un programa de ordenador, siempre que la naturaleza del trabajo preparatorio sea tal que más tarde pueda originar un programa de ordenador».

⁴⁰ En opinión de COTINO HUESO, L., «Caso Bosco...», *cit.*, quien critica la calidad técnica de la resolución, «lo que se alega -y triunfa- por la puerta de atrás es la seguridad informática, que no había sido alegada convenientemente por la Administración cuando tocaba». Los tribunales se basan en diversos informes técnicos para mantener que revelar el código fuente podría comprometer la seguridad de la información y aumentar la vulnerabilidad ante ataques informáticos, lo que podría afectar adversamente la integridad de datos personales y la seguridad pública.

vos, ha sido uno de los más relevantes y criticados por entender la doctrina que la solicitud de transparencia de la Fundación CIVIO estaba más que justificada, ya que no puede tolerarse que se adopten decisiones desestimatorias de beneficios aprobados por el Gobierno en favor de determinados colectivos sin conocer cómo se llega a ellas, lo que genera indefensión y un enorme riesgo de arbitrariedad de los entes públicos⁴¹. Tanto el CTBG estatal como la GAIP, se han pronunciado en diversas ocasiones sobre el acceso al código fuente llegando la mayoría de las veces (aunque no todas) a soluciones favorables al interesado que después han sido anuladas por los órganos jurisdiccionales⁴². Así ocurrió, por ejemplo, en la resolución RT/253/2021 que fue recurrida por la Comunidad de Madrid y el recurso contencioso-administrativo fue estimado por la Sentencia n° 158/2022 del Juzgado Central Contencioso-Administrativo n° 11⁴³.

⁴¹ Criticando la postura adoptada por los distintos órganos y tribunales en este caso, puede verse, entre otros, DE LA NUEZ SÁNCHEZ CASCADO, E., «Algoritmos y transparencia», disponible en <https://www.hayderecho.com/2020/02/18/algoritmos-y-transparencia-2/>, para quien, lo mínimo que se debería exigir es conocer cómo funciona el sistema algorítmico y cómo adopta decisiones que son de enorme relevancia para personas en situación o riesgo de pobreza energética. Para PONCE SOLÉ, J., «A propósito de la sentencia de la Audiencia Nacional de 30 de abril de 2024, núm. de rec. 51/2022, sobre el caso BOSCO», recuperado de Por qué se equivocan las sentencias sobre el algoritmo del bono social eléctrico - Almacén de Derecho (almacenederecho.org), los riesgos aducidos en la sentencia de la Audiencia Nacional conllevarían que pudiera denegarse en cualquier caso el acceso al código fuente, postura que se separa de la que están adoptando otros tribunales de nuestro entorno y órganos administrativos como el CTBG. Criticando también esta postura, COTINO HUESO, L., «Caso Bosco...» *cit.*, y HUERGO LORA, A. (2024) «Por qué aciertan las sentencias sobre el 'algoritmo' del bono social eléctrico», accesible en <https://almacenederecho.org/por-que-aciertan-las-sentencias-sobre-el-algoritmo-del-bono-social-electrico> (último acceso 31 de julio de 2024).

⁴² Pueden verse la Resolución de 21 de septiembre de 2016 de la Comisión de Garantía del Derecho de Acceso a la Información Pública (GAIP), que estima las Reclamaciones 123/2016 i 124/2016 (acumuladas) sobre el algoritmo matemático que determina la selección de los miembros de los tribunales correctores de las pruebas de acceso a la Universidad (PAU) y DNI de los candidatos presentados, y su Resolución 200/2017, de 21 de junio relacionada con las anteriores. Por lo que se refiere al CTBG, las resoluciones R/0058/2021 de 20 de mayo, sobre el acceso al algoritmo para calcular pensiones de la TGSS; RT/253/2021 de 19 de noviembre y RT/ 748/2021 de 10 de enero 2022 sobre acceso al código fuente de aplicación utilizada para el sorteo de tribunales asociados a procesos selectivos para educación en Madrid, y la Resolución del Expediente 551-2023 sobre el acceso a información del Sistema de Seguimiento Integral de los casos de Violencia de Género (Sistema VioGén).

⁴³ El juzgado confirma la aplicación del límite del artículo 14.1.j) de la LTAIBG alegado por la Comunidad para denegar el acceso al código fuente y considera que la petición del solicitante puede considerarse abusiva, vinculando el abuso a su carácter excesivo e injustificado, que excedería del contenido razonable del derecho de acceso a una información pública cabalmente considerado, teniendo en cuenta que el administrado tuvo conocimiento, en todo caso, del funcionamiento del sistema para la designación de los vocales de los tribunales de procesos selectivos cuyo resultado y funcionamiento es público. Por tanto, concluye que en el caso concreto se había dado transparencia al procedimiento público y que los interesados tuvieron la posibilidad de acudir al sorteo público celebrado, teniendo acceso a los resultados de los distintos sorteos al ser públicos.

En relación con el acceso a dicho código, el art. 74.13 RIA aprobado en fechas muy recientes, posibilita que las *autoridades de vigilancia del mercado* (no el público en general) puedan tener acceso al código fuente de los sistemas de alto riesgo, previa solicitud motivada, si se cumplen dos condiciones: a) que dicho acceso sea necesario para llevar a cabo la evaluación de la conformidad del sistema con los requisitos establecidos en el capítulo III, sección 2; y b) que se hubieran agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o estos fueran insuficientes. Ahora bien, como establece el apartado 14, toda la información o documentación a la que tengan acceso tales autoridades de vigilancia deberá ser tratada de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78. Ello con el fin de proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente.

Por último, otro escollo a la transparencia que a su vez dificultaría la averiguación del origen de la discriminación algorítmica, sería la propiedad de los datos utilizados para entrenar al algoritmo⁴⁴. Esta cuestión no es baladí por cuanto los expertos en *machine learning* aseveran que lo realmente útil para detectar el sesgo del sistema podría ser el acceso a los conjuntos de datos que han servido de soporte al aprendizaje del algoritmo⁴⁵. Esto ocurriría en los casos de algoritmos predictivos cuyo aprendizaje se basa precisamente en los datos aportados, a diferencia de lo que ocurriría en los algoritmos no predictivos en los que los datos de alimentación son secundarios; en estos últimos, sí que podría ser útil acceder al código fuente o a la secuencia de programación para averiguar el origen de la decisión, detectando así fallos o errores en alguno de sus pasos⁴⁶.

Hasta hace poco tiempo ninguna norma del acervo comunitario obligaba expresamente a ofrecer acceso a los datos de entrenamiento para investigar posibles errores del sistemas o sesgos discriminatorios⁴⁷. Para LÓPEZ

⁴⁴ RIVAS VALLEJO, P. «Análisis...», *cit.*, pp. 448 y ss. Sobre el derecho de acceso a los datos de entrenamiento de sistema, puede verse ampliamente, LÓPEZ-TARRUELLA MARTÍNEZ, A., *Propiedad intelectual e innovación basada en los datos*, Navarra, 2021, pp. 192 y ss.

⁴⁵ RIVAS VALLEJO, P., «Herramientas desde el derecho antidiscriminatorio y la protección frente a la igualdad y a la no discriminación», p. 548.

⁴⁶ RIVAS VALLEJO, P. «Análisis ...», *cit.*, p. 439.

⁴⁷ Para LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, p. 199, esta laguna podía haberse cubierto mediante una clarificación jurisprudencial o legislativa del derecho de explicabilidad y de su alcance. También considera que podría invocarse el art. 1.2 c) de la Directiva 2016/943 para impedir que el titular de los datos hiciera valer la protección por secreto empresarial para negarse a conceder acceso, al menos en aquellos supuestos en los que el solicitante fuera una autoridad pública. En el acervo comunitario, la fallida *Propuesta de Reglamento sobre un régimen de responsabilidad civil en materia*

TARRUELLA, cuya opinión compartimos, resultaba paradójico que no existiera en el Derecho de la UE una norma de propiedad intelectual que facilitara la investigación de sesgos algorítmicos en general, o de aquellos que pudieran afectar a derechos fundamentales en particular, sobre todo teniendo en cuenta que para las instituciones europeas la transparencia y la explicabilidad eran componentes esenciales de la IA centrada en el ser humano. Para dicho autor, en estos supuestos estaría justificado el acceso a los datos del sistema, e incluso podría considerarse una cuestión de orden público, en tanto que averiguar si la IA discrimina no solo interesa a los particulares afectados sino también a los Gobiernos⁴⁸. Ahora bien, dicho acceso habría que concederlo bajo ciertas salvaguardas que garantizaran, por un lado, los legítimos intereses del titular de los datos, y por otro lado, la protección de la información confidencial⁴⁹.

Pues bien, en fechas recientes se han aprobado diversas normas que garantizan un derecho de acceso a los datos e información algorítmica. Baste citar por el momento, a modo de ejemplo, que la nueva *Ley de Datos* que entró en vigor el 11 de enero de 2024 y será aplicable en septiembre de 2025⁵⁰, establece en su art. 4 el derecho del usuario de un producto o servicio digital contratado a acceder a los datos que el mismo genere. En opinión de NAVAS

de inteligencia artificial, de 20 de octubre de 2020, sí que contemplaba un derecho de acceso a los datos generados por el sistema de alto riesgo (fuesen datos personales o de otro tipo, especialmente técnicos) tanto a la víctima como al operador responsable. Sobre esto el art. 10.2 disponía lo siguiente: «Un operador considerado responsable podrá utilizar los datos generados por el sistema de IA para demostrar la negligencia concurrente de la persona afectada, de conformidad con el Reglamento (UE) 2016/679 y otras leyes en materia de protección de datos relevantes. La persona afectada también podrá usar esos datos con fines probatorios o aclaratorios en la demanda por responsabilidad civil».

⁴⁸ En este sentido, LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, p. 195. Precisamente ese fundamento es el esgrimido en el RIA para justificar el tratamiento de categorías especiales de datos a través de sistemas de IA. Así, evitar la discriminación que podría provocar el sesgo de los sistemas de IA se considera una cuestión de orden público esencial que permitiría que los proveedores trataran ese tipo de datos. De ahí que su art. 10.5 disponga que «*En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas*». Para que se produzca dicho tratamiento deberán cumplirse, además, las condiciones que se establecen en el precepto junto con las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680.

⁴⁹ LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, pp. 195-196. Considera el autor que regulando el acceso a los datos bajo ciertas condiciones se evitaría desincentivar a las organizaciones a invertir en el desarrollo de herramientas de IA ante la posibilidad de verse obligados a compartir los conjuntos de datos en los que se basa su ventaja competitiva. Vid., p. 201.

⁵⁰ Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).

NAVARRO, dicha norma ampara el acceso a los datos a los efectos de una posible futura litigación por daños⁵¹.

No obstante, son las últimas *Propuestas de Directivas de la Comisión Europea*, de 28 de septiembre de 2022, sobre *responsabilidad extracontractual en la IA* y sobre *modernización del régimen de responsabilidad por productos defectuosos* (en adelante, PDRC y PDPD respectivamente)⁵², las que han introducido importantes medidas a fin de remover los obstáculos para acceder a la información algorítmica mediante el reconocimiento de un *derecho a la exhibición de pruebas* a favor de las víctimas. A pesar de su novedad y relevancia, no podemos detenernos en el análisis de dichas normas en este trabajo pues el mismo se centra en otras medidas legislativas. Simplemente apuntaremos que, a nuestro modo de ver, con dicho expediente la Comisión trató de suplir la carencia inicial del RIA respecto a la transparencia externa hacia los afectados por las decisiones de los sistemas de IA, estableciendo un derecho de acceso a la información y a los datos en poder de demandados o potenciales demandados (*vid.*, arts. 3 y 8 respectivamente). El objetivo de esta medida era eliminar los obstáculos con los que podían encontrarse las víctimas para acceder a información del sistema que le permitiera probar los presupuestos para reclamar responsabilidad civil por los daños sufridos e incentivar a proveedores y responsables del despliegue de los sistemas a facilitar información sobre estos y a cumplir las medidas del RIA dirigidas a garantizar la transparencia.

3. TRANSPARENCIA ALGORÍTMICA Y EXPLICABILIDAD: ¿QUÉ IMPLICAN ESTAS EXIGENCIAS?

No es suficiente con requerir que los algoritmos o los sistemas de IA sean transparentes o explicables, sino que hay que determinar qué implican estas exigencias a lo largo de su ciclo de vida y cómo se controlará su cumplimiento.

Aunque en ocasiones ambos términos se emplean como sinónimos, hay que advertir que se trata de dos características distintas de los sistemas de IA, si bien íntimamente conectadas.

Por lo que se refiere concretamente a la transparencia, se ha precisado que es importante distinguir también entre la *transparencia en el ámbito de la IA* y la *transparencia algorítmica*, ya que, mientras la primera se refiere a la «capacidad de entender cómo funcionan los sistemas de IA en general, cómo se

⁵¹ NAVAS NAVARRO, S., *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Granada, 2022, p. 71.

⁵² COM (2022) 496 final (2022/0303(COD)) y COM(2022) 495 final (2022/0302(COD)).

entrenan, cómo toman decisiones y cómo afectan a los usuarios y a la sociedad en su conjunto», la segunda «se centra específicamente en hacer visibles los factores que influyen en las decisiones tomadas por los algoritmos, de modo que puedan ser comprendidos por las personas que utilizan, regulan y se ven afectadas por estos sistemas, siendo su objetivo fundamental garantizar la exactitud y la equidad en las decisiones que afectan a las personas»⁵³.

Según establece la *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*, el principio de transparencia algorítmica «consiste en que siempre ha de ser posible justificar cualquier decisión que se haya adoptado con ayuda de la IA y que pueda tener un impacto significativo sobre la vida de una o varias personas». Es decir, «siempre debe ser posible traducir los cálculos del sistema de inteligencia artificial a una forma comprensible para los humanos», matizándose en otros instrumentos de *soft law* que dicho principio «no consiste en revelar códigos, sino en hacer inteligibles los parámetros y criterios de las decisiones que se toman»⁵⁴. Su finalidad principal es que los usuarios de los sistemas puedan entender su funcionamiento y resultados.

Según el Estudio de Impacto algorítmico del Ministerio de Interior de Países Bajos, la transparencia puede ser tanto *interna* como *externa*. La primera va dirigida principalmente a los sujetos de la cadena de valor de los sistemas (proveedores, responsables del despliegue, importadores, distribuidores, etc.) en beneficio de auditores, supervisores, autoridades o jueces, y es esencial para conocer y comprender su funcionamiento y detectar posibles errores⁵⁵; la segunda, va dirigida al público en general o al menos a todos los

⁵³ FERNÁNDEZ ROZAS, J.C., «La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo», LA LEY Unión Europea, N° 124, Sección Estudios, Abril 2024, LA LEY 15196/2024, p. 24/59. Recuperado de https://www.congreso.es/docu/docum/ddocum/notasdocumentales/nd1/inteligencia_artificial.pdf.

⁵⁴ Así, el Dictamen del CESE sobre *Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa*; la Recomendación del Consejo OCDE sobre IA de 2019 también recoge entre sus principios la exigencia de que los sistemas de IA sean transparentes y explicables lo que implica proporcionar información significativa, adecuada al contexto y coherente; hacer comprensible los sistemas de IA, para que las partes interesadas sean conscientes de sus interacciones con estas herramientas, especialmente en el lugar de trabajo; permitir que los afectados por un sistema de inteligencia artificial entiendan su resultado y puedan cuestionarlo. Vid., p.5/7. Recuperado de: <file:///C:/Users/ASUS/Downloads/db5053b5-93e0-4cf5-a7cf-edce5ee6e893.pdf>. Según el Estándar de Transparencia Algorítmica desarrollado por la Oficina Central Digital y de Datos de Reino Unido, «la transparencia algorítmica significa dar a conocer cómo las herramientas algorítmicas apoyan las decisiones, incluyendo proporcionar información sobre dichas herramientas y las decisiones asistidas por algoritmos en un formato completo, abierto, comprensible, de fácil acceso y gratuito».

⁵⁵ A esta transparencia interna o comunicación de la información entre los distintos sujetos de la cadena de valor de los sistemas se le otorga una especial relevancia a lo largo del RIA, como

interesados o afectados por la IA y también se conoce como «explicabilidad pública»⁵⁶.

La transparencia guarda una estrecha relación con el *principio de explicabilidad*. Así se reconoce, por ejemplo, en la *Recomendación de la UNESCO sobre la ética de la IA de noviembre de 2021*, donde se afirma que ambos conceptos están íntimamente relacionados entre sí, y con la responsabilidad, la rendición de cuentas y la confianza en los sistemas. Además, suelen ser condiciones previas fundamentales para garantizar el respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y los principios éticos. No obstante, como se explica en dicho documento, mientras la *transparencia* pretende proporcionar información para que las personas puedan comprender cómo se implementa cada etapa de un sistema de IA en función de su contexto, conocer los factores que influyen en una predicción o decisión específicas y si existen o no medidas de seguridad o de equidad (e incluso excepcionalmente, en casos de amenazas graves con repercusiones adversas para los derechos humanos, podría exigir que se compartiera el código fuente o los conjuntos de datos utilizados), la *explicabilidad* tiene como objetivo hacer inteligible la entrada, la salida y el funcionamiento de cada componente algorítmico y la forma en que contribuye a los resultados del sistema⁵⁷.

Esta conexión entre la transparencia y la explicabilidad también la pone de relieve el Grupo de Expertos en sus *Directrices éticas para una IA fiable*, donde, además de consagrarse la explicabilidad como uno de los cuatro *principios éticos* que deben respetarse en el desarrollo, despliegue y utilización de los sistemas de IA para garantizar los derechos fundamentales, se incluye como componente fundamental de la transparencia junto con la trazabilidad y la comunicación⁵⁸. No obstante, como aclara el Considerando 49, pese a que

después se explicará. También es a la que se refieren los organismos de normalización técnica NIST (EEUU), ISO, CEN CENELEC (UE).

⁵⁶ Así lo explica COTINO HUESO, basándose en el Estudio citado. Vid., COTINO HUESO, L., «Transparencia de la inteligencia artificial pública: marco legal, desafíos y propuestas», *Actualidad Administrativa*, N° I, Sección Actualidad, Diciembre 2023. Recuperado de La Ley Digital, LA LEY 12767/2023. Para este autor, la transparencia y la explicabilidad permiten comprender resolver problemas técnicos del funcionamiento del sistema, especialmente para comprender la cadena de causalidades.

⁵⁷ Vid., ap.37 a 41.

⁵⁸ *Directrices éticas*, p. 22. COTINO HUESO, L., «Transparencia de la inteligencia artificial pública...», cit., p. 3/23, califica el concepto de transparencia que proporciona el Grupo de expertos en IA de la Comisión Europea en sus *Directrices éticas* como un «concepto inclusivo». Nótese que dicho concepto de transparencia mantenido por el Grupo de Expertos en IA en sus *Directrices éticas*, ha sido el acogido en la versión final del RIA. Así, en el Considerando 27 se establece que, de acuerdo con las citadas Directrices, por transparencia se entiende que «los sistemas de IA se desarrollan y utilizan de un modo que permita una *trazabilidad* y *explicabilidad* adecuadas, y que, al mismo tiempo, *haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente*

numerosas obligaciones legales reflejan principios éticos, el cumplimiento de estos últimos trasciende el mero cumplimiento de las leyes existentes.

Como *principio rector*, se entiende que la explicabilidad «es crucial para conseguir que los usuarios confíen en los sistemas de IA y para mantener dicha confianza» e implica que «los procesos han de ser transparentes, que es preciso comunicar abiertamente las capacidades y la finalidad de los sistemas de IA y que las decisiones deben poder explicarse -en la medida de lo posible- a las partes que se vean afectadas por ellas de manera directa o indirecta», ya que, si no fuera así, se les estaría privando de la posibilidad de presentar alegaciones e impugnarlas adecuadamente⁵⁹.

Como *elemento integrante de la transparencia*, se define como la «capacidad de explicar tanto los procesos técnicos de un sistema de IA, como las decisiones humanas asociadas» y se establece que dicha exigencia requiere que las decisiones del sistema «sean comprensibles para los seres humanos y estos tengan la posibilidad de rastrearlas»⁶⁰.

El *grado* de explicabilidad exigible va a depender en gran medida del contexto en el que se enmarquen estos sistemas y de la gravedad de las consecuencias derivadas de un resultado erróneo o impreciso (por ejemplo, un sistema de IA que genere unas recomendaciones de compra poco acertadas no será preocupante desde el punto de vista ético, a diferencia de uno dirigido a evaluar la concesión de la libertad condicional al condenado) y debe ser *suficiente* para poder impugnar los resultados y solicitar un resarcimiento por los daños que se generen⁶¹. Además, en la medida de lo posible, la explicabilidad debe estar adaptada a las personas afectadas⁶².

a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos». Este Considerando 27 contiene lo dispuesto en la enmienda 213 del Parlamento europeo que proponía un nuevo art. 4 bis donde se recogieran los «Principios generales aplicables a todos los sistemas de IA», en cuyo apartado 1. d) figuraba la transparencia.

⁵⁹ Vid., ap. 53 *Directrices éticas*.

⁶⁰ P. 22.

⁶¹ Así lo afirma el Parlamento Europeo en la Propuesta de Reglamento que acompañaba a su Resolución sobre aspectos éticos de la IA, de 20 de octubre de 2020. Vid., Considerando 19, donde finaliza diciendo que «La auditabilidad, la trazabilidad y la transparencia deben tratar cualquier posible ininteligibilidad de estas tecnologías». La UNESCO en su *Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO* (2021), señala que dicho grado de transparencia deberá ajustarse al contexto y efecto del sistema de IA.

⁶² Vid., Comunicación de la Comisión Europea «Generar confianza en la inteligencia artificial centrada en el ser humano» (COM/2019/168 final), p. 6 o *Directrices éticas* del Grupo de Expertos, p. 22, donde se apunta que la explicación «debería ser oportuna y adaptarse al nivel de especialización de la parte interesada (que puede ser una persona no experta en la materia, un regulador o un investigador)».

Para COTINO HUESO, las variables que podrían condicionar el grado o intensidad de explicabilidad y transparencia exigible serían las siguientes: en primer lugar, el impacto que tiene el algoritmo en la decisión, el resultado y el ciudadano; en segundo lugar, el grado de autonomía del sistema en la toma de decisiones (es decir, hasta qué punto se garantiza la participación humana); y por último, el tipo y la complejidad del algoritmo. Así, cuanto mayor sea el impacto de las decisiones algorítmicas en los ciudadanos y mayor sea la autonomía, opacidad y complejidad del sistema de IA, mayores niveles de transparencia y explicabilidad se tendrán que exigir⁶³.

Por lo que se refiere a los algoritmos de *black box*, en los que no es posible obtener una explicación acerca de cómo se ha generado un resultado determinado o qué combinación de *inputs* han contribuido al mismo, la explicabilidad debe traducirse en medidas como la trazabilidad, la auditableidad o la comunicación transparente de las capacidades del sistema para que las personas afectadas puedan comprender cuál es la base de sus acciones o decisiones⁶⁴. Es decir, en tales casos es necesario adoptar otro tipo de estrategias de control con el fin de desarrollar sistemas algorítmicos explicables desde un punto de vista práctico. Más allá de la apertura de la caja negra (que como hemos visto no siempre será la panacea para la víctima), la doctrina ha venido manteniendo que dichas estrategias debían ir dirigidas al escrutinio de los datos de entrada y salida y al establecimiento de una serie de garantías en el proceso de diseño, entrenamiento e implementación de los sistemas y de procedimientos de monitorización y supervisión de los resultados. Garantías y procedimientos que, además, debían someterse a auditorías⁶⁵. Como iremos viendo a lo largo de estas páginas, muchas de estas estrategias han sido recogidas en el nuevo Reglamento europeo sobre IA.

⁶³ Así lo entiende COTINO HUESO, L., «Transparencia de la inteligencia artificial pública...», cit. También en «Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida» *Revista Española de la Transparencia*, Núm. 16, 2023, pp.17-63, accesible en file:///C:/Users/ASUS/Downloads/Dialnet-QueConcretaTransparenciaEInformacionDeAlgoritmo sEI-8913030.pdf

⁶⁴ La Comisión Europea ha señalado en diversos documentos que en relación a aquellas aplicaciones de IA que entrañan un riesgo elevado, el marco regulador podrá exigir la conservación de registros exactos sobre el conjunto de datos utilizados para entrenar el algoritmo, una descripción de sus principales características y del modo en que se escogió, así como de documentación sobre las metodologías de programación y entrenamiento y los procesos y las técnicas utilizados para construir, probar y validar los sistemas; además de obligar a facilitar información clara de sus capacidades y limitaciones, objetivo y condiciones en las que se espera que funcione según lo previsto. Incluso considera el diseño de *sistemas mixtos* que combinen redes neuronales profundas y razonamiento simbólico (esto es, reglas creadas mediante intervención humana) como una solución técnica que ayude a mejorar la capacidad de explicar los resultados de la IA. Vid., *Directrices éticas* p. 16 y también el *Libro Blanco sobre la inteligencia artificial* (COM (2020) 65 final), pp. 23-25.

⁶⁵ Por todos, SOLAR CAYÓN, J.I., *op.cit.*, p. 152.

Además de la explicabilidad, la transparencia incluye también la *trazabilidad* y la *comunicación*⁶⁶. Esto significa que no sólo se debe poder reconstruir cómo y por qué un sistema se comporta de determinada manera, sino que quienes interactúen con ellos deben saber que no se trata de un humano sino de un sistema inteligente y qué personas responderán de sus acciones o decisiones.

A mayor abundamiento, la transparencia también debe aplicarse a los elementos del sistema de IA, es decir, los datos, el *software* y los modelos de negocio⁶⁷. Para conseguirla, deben documentarse los conjuntos de datos y procesos que dan lugar a la decisión del sistema, incluidos los relativos a la recopilación y etiquetado de datos, estar disponibles las explicaciones sobre el grado en que un sistema de IA condiciona e influye en el proceso de toma de decisiones de la organización, las opciones de diseño de dicho sistema y la justificación de su despliegue⁶⁸. En relación a este último extremo, algunos estudios advierten que puede haber otros problemas de transparencia que no estén relacionados con el algoritmo en sí mismo o con los datos que utiliza, sino con la falta de claridad en cuanto a las razones por las que se usa un determinado sistema de IA y los objetivos que persigue. En Francia, por ejemplo, el algoritmo *Parcoursup*, que se utilizaba para asignar a los estudiantes a las universidades, fue muy criticado porque sus objetivos no estaban bien definidos⁶⁹.

Respecto a los datos, cuando estos sistemas empleen datos *personales* será de obligada aplicación el RGPD, en cuyo contexto la transparencia se configura como una obligación para los responsables del tratamiento a la hora de comunicar determinada información al interesado, lo que debe hacerse de forma «concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo» según dispone su art. 12.1. De ahí que se infiera que la principal preocupación del RGPD es la transparencia «hacia la persona interesada», más allá de las posibles soluciones técnicas para ayudar a esclarecer lo que hasta el momento es inescrutable⁷⁰.

⁶⁶ Sobre ambas características, vid., *Directrices éticas*, p. 22.

⁶⁷ *Ibidem*. También la Agencia Europea de los Derechos Fundamentales mantiene que, tanto la transparencia como las evaluaciones de impacto, deben verificarse tanto sobre la calidad de los datos, como sobre la forma en que funcionan los algoritmos (caja negra) y las facultades predictivas de los mismos. Vid., EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), «BigData: Discrimination in data-supported decision making» 2018.

⁶⁸ Vid., Comunicación de la Comisión Europea «Generar confianza en la inteligencia artificial centrada en el ser humano» (COM/2019/168 final), p. 6.

⁶⁹ GERARDS, J./ XENIDIS, *op.cit.*, p. 87.

⁷⁰ LAZCOZ MORATINOS, G., *op.cit.*, p. 296.

Sin embargo, como apunta la AEPD, en los casos de *tratamientos de datos basados en IA* (esto es, cuando los sistemas de IA se incluyen en, o son medios de, un tratamiento de datos personales) «la transparencia debe permitir a los interesados ser conscientes del impacto que el empleo de dichas soluciones puede llevar asociado y de ahí que la transparencia esté dirigida tanto a los interesados como a los operadores del tratamiento, y que esté ligada, en particular, con una *información veraz sobre la eficiencia, las capacidades y las limitaciones reales de los sistemas de IA, que evite la creación de falsas expectativas, en los usuarios y los interesados, que puedan ocasionar una mala interpretación de las inferencias que se realizan en el marco del tratamiento. También, la transparencia está ligada a información sobre el contexto y situación del tratamiento, como la existencia de terceras partes, la localización física/virtual de la solución AI, etc*». En tales casos, los responsables del tratamiento deben obtener suficiente información sobre los sistemas para cumplir con las obligaciones que les impone el RGPD y que incluyen la transparencia para permitir el ejercicio de los derechos, el cumplimiento del principio de responsabilidad activa, o cumplir los requisitos de las Autoridades de Supervisión en relación con sus poderes de investigación y de los organismos de certificación y supervisión de códigos de conducta. Además, como sigue diciendo la AEPD, «[l]a transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución»⁷¹.

Por tanto, es importante percatarse ya de entrada de que la transparencia tiene diferentes implicaciones en el RIA y en el RGPD en la medida en que afecta a distintos actores, se refiere a información diferente y va dirigida a diferentes destinatarios⁷². Como después se detallará, en el RIA la transparencia es exigible desde el diseño del sistema y a lo largo de todo su ciclo de vida independientemente de si el mismo procesa o no datos personales. Va referida a los sistemas en sí mismos y las obligaciones que de ella derivan van dirigidas a diseñadores, desarrolladores, proveedores y responsables del despliegue. Por su parte, la transparencia recogida en el RGPD se aplica a los tratamientos de datos personales definidos en los arts. 2 y 4.2 y las obligaciones que implica recaen sobre los responsables de dicho tratamiento. No obstante, como aclara la AEPD, «los *diseñadores y desarrolladores* pueden ser responsables o encargados del tratamiento si utilizan datos personales en el diseño o desa-

⁷¹ Informe de la AEPD sobre la *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, p. 33

⁷² Como explica la AEPD en <https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia>, el RIA (cuyo ámbito material son los sistemas de IA) establece un concepto de transparencia que difiere del mismo término establecido en el RGPD (cuyo ámbito material son los tratamientos de datos personales).

rollo del sistema de IA. Los *proveedores* pueden ser responsables o encargados del tratamiento si los sistemas de IA almacenan o tratan datos de interesados identificados o identificables. [Y] los *usuarios/entidades que despliegan* un sistema de IA podrían ser responsables o encargados del tratamiento si incluyen dicho sistema como parte de sus tratamientos»⁷³. En cualquier caso, sólo aquellos que actúen como responsables del tratamiento quedarán sujetos a las obligaciones de transparencia del RGPD.

Por último, cabe señalar también que la transparencia a la que se refiere el RIA se dirige principalmente a los responsables del despliegue y está relacionada con la explicabilidad, documentación, mantenimiento de registros e información sobre cómo utilizar dicho sistema de IA⁷⁴, mientras que los destinatarios de las obligaciones de transparencia derivadas del RGPD son los interesados -personas físicas- y su contenido mínimo se recoge en los arts. 13 y 14 RGPD. No obstante, como también se explicará con detenimiento después, aunque el RIA abogue principalmente por la transparencia interna, también establece obligaciones a favor de la transparencia externa y ha acabado incorporando, como novedad relevante respecto a su versión inicial, el *derecho a una explicación* de las personas afectadas por las decisiones algorítmicas.

4. MEDIDAS PARA GARANTIZAR LA TRANSPARENCIA Y LA EXPLICABILIDAD EN LA TOMA DE DECISIONES ALGORÍTMICAS

4.1 ESTADO DE LA CUESTIÓN

Hasta hace poco tiempo el único instrumento para hacer frente a la opacidad de los sistemas automatizados de decisiones, basados o no en IA, era el RGPD. Sin embargo, en los últimos años se han presentado otras propuestas

⁷³ <https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia>. Sobre esto, el Considerando 10 RIA señala que el Reglamento no afectará a las obligaciones de los proveedores y responsables del despliegue en su papel de responsables o encargados del tratamiento si el diseño, desarrollo o uso del sistema IA implica tratamiento de datos personales. Las normas armonizadas del RIA deberán facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el Derecho de la Unión en materia de protección de datos personales, así como de otros derechos fundamentales.

⁷⁴ Vid., por ejemplo, el art. 13 y el Considerando 72, donde se da amplia cuenta de que la transparencia exigible a los sistemas de IA de alto riesgo va dirigida, principalmente, a que los responsables del despliegue puedan «comprender la manera en que el sistema de IA funciona, evaluar su funcionalidad y comprender sus fortalezas y limitaciones», así como «utilizar el sistema y tomar decisiones con conocimiento de causa».

regulatorias por las instituciones europeas y se han ido aprobado paulatinamente normas a nivel interno y comunitario, tendentes a garantizar en mayor o menor medida la transparencia algorítmica y el derecho a una explicación, esto es, el derecho a conocer cómo funciona el concreto proceso de toma de decisión con indicación de los datos específicos de la persona en base a los cuales se ha tomado una decisión o se ha hecho un perfilado⁷⁵. El objetivo de todas ellas es eliminar, o al menos mitigar, la opacidad tanto en el *uso* como en el *contenido* de la información sobre el algoritmo y se asientan sobre una serie de principios como el de transparencia desde el diseño, minimización de sesgos y rendición de cuentas⁷⁶.

⁷⁵ Más allá del RGPD, a nivel europeo contamos con algunas normas que regulan y exigen transparencia algorítmica en ámbitos concretos. Por ejemplo, respecto a las plataformas que prestan servicios de intermediación en línea, el *Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea* (conocido como Reglamento P2B), que obliga a plataformas y motores de búsqueda a dar publicidad a los parámetros principales de funcionamiento de sus algoritmos de prelación de ofertas (arts. 5 y 7). Por otro lado, la *Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo*, en lo que atañe a la mejora de la aplicación y modernización de las normas de protección de los consumidores de la Unión, establece que los comerciantes pueden personalizar el precio de sus ofertas para determinados consumidores o determinadas categorías de consumidores basándose en la toma de decisiones automatizada y la elaboración de perfiles a partir de su comportamiento, pero en tales casos se les deberá informar acerca de los principales parámetros por defecto que determinan la clasificación de las ofertas mostradas y su importancia relativa frente a otros parámetros, a fin de que puedan tener en cuenta los riesgos potenciales de su decisión de compra. También en muchos instrumentos de *soft law* provenientes de la UE se aboga por la transparencia, información y explicabilidad de los sistemas algorítmicos. Vid., por ejemplo, las *Resoluciones del Parlamento Europeo de 12 de febrero de 2020 sobre los procesos automatizados de toma de decisiones*, o la de *20 de octubre de 2020 sobre aspectos éticos de la IA*. Y también contamos en el ámbito europeo con un reconocimiento de derechos digitales del que se desprende el derecho a conocer que estamos siendo objeto decisiones algorítmicas. Se trata de la *Declaración sobre los Derechos y Principios Digitales*, de 23 de enero de 2023, donde se recoge el compromiso de «velar por un nivel adecuado de transparencia en el uso de los algoritmos y la inteligencia artificial y porque las personas estén informadas y capacitadas para utilizarlos cuando interactúen con ellos».

⁷⁶ Particularmente relevante en el tema que nos ocupa es la *Ley 15/2022 integral de igualdad*, que en su art. 23, establece el deber de las administraciones públicas de poner en marcha mecanismos para que los algoritmos involucrados en la toma de decisiones tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, y que se priorice la transparencia en el diseño y la implementación, así como la capacidad de interpretación de las decisiones adoptadas por los mismos, precepto que, no obstante su relevancia a la hora de sentar parámetros generales, ha sido considerado por la doctrina como una mera declaración de intenciones que deberá concretarse en medidas específicas a cumplir por las administraciones y las empresas. En el ámbito público, algunas leyes de transparencia autonómicas ya recogen deberes de información en relación con el uso de algoritmos. Así, la pionera *Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunidad Valenciana*, en su art. 16 (letra l). Por otro lado, y aunque no tiene carácter vinculante, la *Carta de Derechos Digitales* española reconoce a los ciudadanos una serie de derechos frente a la Administración cuando se utilicen sistemas inteligentes en la toma de decisiones, que se traducen en cargas o deberes de información y transparencia para los entes públicos (*vid.*, ap.XVIII.6). En el

Además, contamos con pronunciamientos judiciales y de órganos administrativos que se posicionan a favor de garantizar un nivel de transparencia algorítmica mucho mayor y obligaciones de información más exigentes en los casos en que los sistemas de IA para la automatización de decisiones se utilicen en el ámbito público⁷⁷. Todo ello contribuye, sin duda alguna, a luchar contra algunos de los principales obstáculos que plantea la discriminación algorítmica como son su detección y prueba.

Asimismo, todas las soluciones propuestas o aprobadas pretenden garantizar la transparencia algorítmica sin afectar a los derechos de autor y los secretos empresariales. De hecho, encontrar un equilibrio entre la propiedad intelectual de ciertos métodos de procesamiento y la necesidad de garantizar la transparencia, imparcialidad y equidad algorítmica, ha sido considerado por las instituciones europeas como un objetivo imprescindible desde que comenzaron a trabajar sobre la IA hasta sus más recientes y relevantes propuestas normativas⁷⁸.

De todas las medidas legales para hacer frente a la opacidad de los sistemas de IA, en el presente trabajo nos centraremos en las contenidas en el RGPD y en el RIA. Por lo que se refiere al RIA, su reciente aprobación y la importancia de las medidas que contiene respecto a la transparencia algorítmica y la explicabilidad, justifican sobradamente que le dediquemos una atención

Derecho laboral español, junto con la conocida como *Ley Rider* (a la que haremos referencia posteriormente), otra norma con la que se trata de hacer frente a la opacidad algorítmica y fomentar la transparencia de la IA es la *Ley 3/2023, de 28 de febrero, de Empleo*. Dicha norma establece la creación de herramientas de apoyo a la toma de decisiones basadas en evidencias estadísticas para la mejora de la empleabilidad de las personas. En concreto, es el art. 17 el que se ocupa de la «toma de decisiones fundamentada en el análisis de datos, las evidencias estadísticas y el análisis del mercado de trabajo».

⁷⁷ Además de la sentencia de 5 de febrero de 2020 del Tribunal de lo Civil de la Haya dictada en el caso del algoritmo Syri, también se obligó a dar acceso al código fuente de diferentes sistemas automatizados empleados por el sector público en los siguientes asuntos: Tribunal Regional Administrativo del Lazio-Roma, Sección III bis, Sentencias N° 3769, de 22 de marzo de 2017 y N° 10964, de 13 de septiembre de 2019; Comisión Francesa de Acceso a los Documentos Administrativos, Decisiones N° 20144578, de 8 de enero de 2015 y N° 20180276, de 19 de abril de 2018. En nuestro país, la Resolución de 21 de septiembre de 2016 de la Comisión de Garantía del Derecho de Acceso a la Información Pública (GAIP), que estima las Reclamaciones 123/2016 i 124/2016 (acumuladas) sobre el algoritmo matemático que determina la selección de los miembros de los tribunales correctores de las pruebas de acceso a la Universidad (PAU) y DNI de los candidatos presentados, y su Resolución 200/2017, de 21 de junio relacionada con las anteriores. Por lo que se refiere al CTBG, las resoluciones R/0058/2021 de 20 de mayo, sobre el acceso al algoritmo para calcular pensiones de la TGSS; RT/253/2021 de 19 de noviembre y RT/ 748/2021 de 10 de enero 2022 sobre acceso al código fuente de una aplicación utilizada para el sorteo de tribunales asociados a procesos selectivos para educación en Madrid, y la Resolución del Expediente 551-2023 sobre el acceso a información del Sistema de Seguimiento Integral de los casos de Violencia de Género (Sistema VioGén).

⁷⁸ Vid., por ejemplo, el art. 78 RIA; el Considerando 20 y el art. 3.4 PDRC; y los Considerandos 31 y 32 y art. 8 apartados 2,3 y 4 PDPD.

especial. Por lo que respecta al RGPD, la novedosa jurisprudencia sentada por el TJUE sobre su art. 22, precepto básico y fundamental para hacer frente a los riesgos del *machine learning* en la toma de decisiones basadas en datos personales, hace que sea necesario analizar con particular detenimiento dicho precepto y su interacción con el nuevo art. 86 RIA.

4.2 LA TRANSPARENCIA Y LA EXPLICABILIDAD EN EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, DE PROTECCIÓN DE DATOS (RGPD): ESPECIAL REFERENCIA A LAS DECISIONES AUTOMATIZADAS DEL ART. 22

Los principios sobre los que se asienta el RGPD⁷⁹, recogidos en su art. 5 y entre los que se encuentra el de transparencia, obligan a responsables y encargados del tratamiento a comunicar al interesado cómo y por qué se recogen y utilizan sus datos personales, así como a garantizar su exactitud, entre otras cosas. En virtud del principio de transparencia, desarrollado en los Considerandos 39 y 58, debe quedar totalmente claro para las personas físicas que se están recogiendo, utilizando, consultando o tratando de otra manera sus datos personales, así como la medida en que dichos datos son o serán tratados. Además, toda la información y comunicación relativa al tratamiento debe ser fácilmente accesible y fácil de entender, utilizando un lenguaje sencillo y claro y, en su caso, visualizándose⁸⁰.

Más allá de las exigencias derivadas del citado principio, el RGPD establece una serie de garantías y derechos para hacer frente a la opacidad algorítmica cuando el interesado es objeto de una decisión plenamente automatizada basada en sus datos personales y con efectos jurídicos o similares en él: por un lado, los arts.13.2 f), 14.2 g) y 15.1.h) obligan a informarle sobre la *existencia de decisiones automatizadas*, incluida la elaboración de perfiles, y al menos en tales casos, a darle *información significativa sobre la lógica aplicada, así como la importancia y las consecuencias que dicho tratamiento puede tener para su persona*. Por tanto, se consagra un derecho de información reforzado o ampliado exigible cuando concurren los presupuestos mencionados; por otro lado, el art. 22.3 establece que, en tales casos, el responsable del tratamiento adoptará las

⁷⁹ Dichos principios son: licitud, lealtad y transparencia (art. 5.1.a); limitación de la finalidad (art.5.1.b); minimización de datos (art. 5.1.c); exactitud (art. 5.1.d); limitación del plazo de conservación (art. 5.1.e); integridad y confidencialidad (art. 5.1.f); y responsabilidad proactiva (art. 5.2).

⁸⁰ Se destaca también en el Considerando 58 que la transparencia «es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea».

medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, y, como mínimo, el *derecho a obtener intervención humana* por parte del responsable, a *expresar su punto de vista* y a *impugnar la decisión* que le afecta.

No hay unanimidad acerca de si el RGPD consagra un «derecho de explicabilidad algorítmica» o «derecho a abrir la caja negra de los algoritmos». Mientras el derecho de información *ex ante* está adecuadamente regulado en el RGPD -como se deriva de los arts. 5.1, 13, 14 o 15 que acabamos de mencionar- y parece claro que opera con anterioridad a que el sistema adopte la decisión o haga el perfilado, se discute su existencia *ex post*, esto es, después de elaborada la decisión o el perfil de la persona. La controversia se basa, principalmente, en que dicho derecho no se reconoce en el texto articulado sino simplemente en uno de sus considerandos, en concreto en el número 71, según el cual, el afectado por la decisión automatizada goza del «derecho a obtener intervención humana, a expresar su punto de vista, a recibir una *explicación de la decisión tomada después de tal evaluación* y a impugnar la decisión»⁸¹. Teniendo en cuenta que los considerandos no son en sí mismos normas, si la concreta decisión o el perfilado adoptados por el sistema perjudican al interesado, no hay consenso acerca de si éste tendría derecho a que se le informara sobre la *lógica decisional* (distinta de la *lógica aplicada* a la que se refieren los art. 13,14 y 15⁸²), es decir, a que se le explicara el proceso decisorio que ha

⁸¹ Sobre esta controversia doctrinal, puede verse LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, pp. 197 y ss, y doctrina citada en notas 718 y 719. También sobre el asunto, NÚÑEZ SEOANE, J., «El derecho a la información y acceso al funcionamiento de los algoritmos que tratan datos personales», en *La regulación de los algoritmos*, coord. por Gustavo Manuel Díaz González y Alejandro José Huergo Lora (dir.) 2020, pp.307-308.

⁸² Diferencia con claridad entre lo que sería la lógica aplicada y la lógica decisional, GIL MEMBRADO, C., «Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra», en N. Álvarez Lata/J.M. Busto Lago, *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, 2024, p. 521. La primera estaría reconocida en los arts. 13 y 14 RGPD y obligaría a informar sobre el sistema de IA en general, mientras que la segunda obligaría a abordar qué proceso decisorio ha conducido a un determinado resultado de salida. En su opinión, el RGPD sólo reconoce la primera (esto es, el derecho a conocer la lógica aplicable -*ex ante*-, pero no el derecho a conocer la explicabilidad -*ex post*-). Para MEDINA GUERRERO, M., «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales», *Teoría y realidad constitucional*, n° 49, 2022, p. 161, el deber de proporcionar «información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas» previsto en los arts. 13.2.f) y 14.2.g) RGPD, sólo puede traducirse en la práctica en una explicación *ex ante* sobre la *funcionalidad del sistema* en la medida en que debe llevarse a cabo en el momento en que se obtengan los datos personales (ex art. 13.2) o en un plazo muy breve (ex art. 14.3.a). Al realizarse la notificación antes de que el sistema decisional haya adoptado la solución concreta, la información que debe dar el responsable no puede relacionarse con el resultado de ninguna decisión específica, sino que deberá centrarse en el sistema considerado como un todo abstracto. Por lo que, como es lógico, en esta fase la obligación de información no puede traducirse en la exigencia de asegurar la explicabilidad o la fundamentación de una decisión en particular. Y en sentido similar,

conducido a que el sistema arrojará ese resultado concreto, así como si este derecho incluiría, a su vez, el derecho a acceder a los datos de entrenamiento del sistema.

La cuestión no es baladí si se tiene en cuenta que la solicitud de un interesado para investigar posibles errores o sesgos discriminatorios de la IA se producirá siempre *ex post*, es decir, una vez adoptada la decisión discriminatoria⁸³. Para un sector doctrinal, al que nos adherimos, se podría defender la existencia de este derecho a la explicabilidad *en ambos momentos*. Una interpretación sistemática de los derechos de información de los arts. 13, 14 y 15, junto con los derechos del art. 22.3 y el Considerando 71, implicaría reconocer que el derecho a la explicación está incorporado siquiera implícitamente en el art. 22.3⁸⁴. Así lo mantiene entre nuestros autores NÚÑEZ SEOANE para quien no cabe duda de que se reconoce este derecho en ambas sedes teniendo en cuenta que es el resultado o consecuencia del ejercicio por el interesado de los previos derechos o garantías a la intervención humana y a formular las alegaciones que prevé el artículo 22.3; así, una vez solicitada la intervención humana y formuladas las alegaciones pertinentes, el responsable deberá ofrecer «una explicación de la decisión tomada después de tal evaluación» a la que se refiere el Considerando 71, ya que solo después de que sus alegaciones hayan

apunta PALMA ORTIGOSA, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos», *Revista General de Derecho Administrativo*, n. 50, 2019, p. 14/25, que «el derecho a la explicación exige del responsable una aportación de información mucho más personalizada sobre la decisión algorítmica que aquella que debía aportar en un primer momento el responsable conforme a los Arts. 13.2.f), 14.2.g), 15.1.h) RGPD, información previa que no tenía todavía en cuenta la decisión automatizada del particular basada en los datos personales aportados por este último».

⁸³ LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, p. 197.

⁸⁴ En este sentido, SELBST, A. D./POWLES, J., «Meaningful information and the right to explanation», *International Data Privacy Law*, Vol. 7, n.º 4, 2017, pp.233 y ss, GOODMAN, B./FLAXMAN, S., «European Union regulations on algorithmic decision-making and a “right to explanation”» presented at ICML Workshop on Human Interpretability in Machine Learning, New York, 2016, <https://arxiv.org/abs/1606.08813v3>; BIBAL A./LOGNOUL, M./DE STREEL, A./FRÉNAY, B., «Legal requirements on explainability in machine learning», *Artificial Intelligence & Law*, 29(2), 2021, pp. 149-169. También entre nuestros autores, NAVAS NAVARRO, S., *Daños ocasionados ...*, *cit.*, p. 72, NÚÑEZ SEOANE, J., «El derecho a la información y acceso al funcionamiento de los algoritmos que tratan datos personales», en *La regulación de los algoritmos*, coord. por Díaz González y Huergo Lora (dir.) 2020, LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.loc.cit.* En sentido contrario, la falta de refrendo legal y el carácter no vinculante de los considerandos, ha llevado a otro sector doctrinal a entender que en el RGPD no existe un derecho de explicabilidad. Manteniendo esta última postura, WACHTER, S., MITTELSTADT, B., y FLORIDI, L., «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», *International Data Privacy Law*, Vol. 7, n. 2, 2017. Estos autores afirman que la omisión del derecho a la explicación en el artículo 22.3 es intencionada, por lo que niegan su reconocimiento. También, en nuestra doctrina, GIL MEMBRADO, C., *op.cit.loc.cit.*, considera que el RGPD no reconoce el derecho a la explicabilidad *ex post*.

sido revisadas, evaluadas y explicadas por una persona, podrá ejercer en condiciones su derecho de impugnación⁸⁵.

Junto con las vacilaciones acerca de la propia *existencia* del derecho a la explicabilidad, también se ha discutido (y criticado) su *alcance y contenido*. Determinar cuándo opera este derecho obliga a analizar con más detalle el art. 22 RGPD por cuanto los derechos y garantías mencionadas se aplican sólo en los casos de decisiones individuales automatizadas y perfilados a que éste se refiere.

4.2.1 Ámbito de aplicación del art. 22 RGPD

El art. 22 RGPD es el punto de enlace entre la IA y la protección de datos, puesto que las decisiones automatizadas y la elaboración de perfiles son dos de sus aplicaciones más frecuentes⁸⁶. Se trata de uno de los pocos preceptos que prevé una serie de garantías jurídicas en los casos en que se adopten decisiones automatizadas, ya sea mediante sistemas de IA o no. Por tanto, si el tratamiento de datos personales, la elaboración de perfiles o la toma de decisiones sobre una persona física es realizada por un componente IA, tendrá que someterse al RGPD. En caso contrario, esto es, si no se tratan datos personales, no será necesario. El problema reside en que en muchos casos no es sencillo determinar si durante una etapa del ciclo de vida de un sistema basado en IA se tratan o no datos personales⁸⁷.

Tanto el ámbito de aplicación del art. 22, como los derechos y garantías que implica y su concreta efectividad cuando la automatización de decisiones se lleva a cabo a través de sistemas de IA, han sido objeto de críticas y comen-

⁸⁵ NÚÑEZ SEOANE, J., *op.cit.*, p. 308

⁸⁶ HERRERA DE LAS HERAS, R., «Protección de datos e inteligencia artificial», en Cruz Blanca/Lledó Benito (coords.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, 2021, p. 654. No obstante, como matiza REBOLLO DELGADO, L. *Inteligencia artificial y derechos fundamentales*, Madrid, 2023, p. 107, estas dos funcionalidades hoy en día ya no son troncales de la IA y la aplicación del precepto únicamente a ellas se manifiesta claramente insuficiente teniendo en cuenta la amplitud de posibilidades que ofrece la IA. Para una explicación detallada sobre las diferencias entre estas dos figuras jurídicas recogidas en el RGPD que guardan relación con los procesos de tratamiento de datos y que dan lugar a inferencias o predicciones sobre comportamientos o preferencias de las personas, puede verse LAZCOZ MORATINOS, G., *op.cit.*, p. 288. Baste mencionar aquí que las decisiones automatizadas tienen un ámbito de aplicación que puede solaparse parcialmente con la elaboración de perfiles o derivar de ésta. En ocasiones, la toma de decisiones automatizada requiere previamente la elaboración del perfil de la persona intentando hacer una predicción sobre sus características o comportamiento; en otros casos, la decisión se toma sobre la base de datos referentes a la actividad de la persona sin necesidad de elaborar un perfil.

⁸⁷ Así lo afirma la AEPD, *Adecuación...*, cit., p.14.

tarios por la doctrina⁸⁸. Además, en fechas muy recientes, el TJUE se ha pronunciado por primera vez sobre el ámbito de aplicación de dicho precepto, en su sentencia de 7 de diciembre de 2023, asunto C-634/21 (*OQ y Land Hessen, con intervención de SCHUFA Holding AG*), sentando doctrina importante al respecto. Es conveniente, por ello, detenerse en el análisis de tales cuestiones.

La primera garantía que recoge el art. 22 RGPD consiste, precisamente, en *prohibir con carácter general que las personas puedan ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos personales*, incluyendo la elaboración de perfiles, *siempre que dichas decisiones produzcan efectos jurídicos sobre ellas o les afecten significativamente de modo similar* (art. 22.1). No obstante, se establecen una serie de casos en los que excepcionalmente se permiten dichas decisiones y que restan eficacia a la prohibición, a saber: a) que sean necesarias para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) que estén autorizadas por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; y c) que el interesado haya dado su consentimiento explícito. Analizaremos a continuación tanto las excepciones como la regla general contenida en el precepto.

A) *Excepciones*

La primera excepción plantea muchas dudas interpretativas acerca de cuándo «es necesaria» una decisión de este tipo para la celebración o ejecución de un contrato, ya que lo normal es que el uso de sistemas para automatizar decisiones responda a razones de conveniencia de una de las partes, más que de necesidad⁸⁹. Además, la «necesidad» debe interpretarse de manera estricta, lo que significa que el tratamiento automatizado debe ser esencial para poder perfeccionar el acuerdo o cumplir con las obligaciones contractuales. Así, esta base de legitimación podrá alegarse en sectores u organiza-

⁸⁸ Por todos, PALMA ORTIGOSA, A., *op.cit.*, y REBOLLO DELGADO, L., *op.cit.*, pp. 101 y ss. También afirma con rotundidad OTTOLIA, A., *Derecho, Biga Bata e Inteligencia Artificial*, Valencia, 2018, p.102, que «[...] la aplicación real del precepto es decepcionante, ya que resulta debilitado por las excepciones que prevé».

⁸⁹ HUERGO LORA, A., «Una aproximación a los algoritmos desde el derecho administrativo», en A. HUERGO LORA (dir.) y G. DÍAZ GONZÁLEZ (coord.), *La regulación de los algoritmos*, Navarra, 2020, p. 62. De hecho, el GT 29 reconoce en sus *Directrices sobre decisiones individuales automatizadas*, cit., p. 26, que los responsables del tratamiento pueden, con fines contractuales, acudir a los procesos de decisiones basadas únicamente en el tratamiento automatizado de datos por considerar que es la mejor manera de conseguir un determinado objetivo, ya que «la participación humana rutinaria puede resultar poco práctica o imposible debido a la magnitud de los datos tratados».

ciones donde es habitual realizar una evaluación previa del interesado que pretende formalizar un contrato con el responsable. Piénsese por ejemplo en sectores como el bancario, el de seguros o el laboral. De hecho, en el caso de la concesión de créditos es obligatorio realizar una evaluación previa de la solvencia patrimonial del solicitante⁹⁰. Para ello, el responsable, antes de concertar dicho contrato, valorará al interesado con el objetivo de analizar la viabilidad futura del acuerdo. En definitiva, lo realmente importante para que se pueda aplicar esta base legitimadora del tratamiento es que el responsable demuestre que no hay otro método igualmente efectivo y menos invasivo para la intimidad con el que se pueda lograr el mismo objetivo. Si lo hubiera, dicho tratamiento no podría calificarse de «necesario»⁹¹.

Respecto a la segunda excepción, parece que se permiten las decisiones plenamente automatizadas cuando estén autorizadas legalmente, es decir, se permite que el Derecho de la UE o de los Estados miembros pueda establecer normas donde se autorice a los responsables a llevar a cabo este tratamiento automatizado de datos personales para la toma de decisiones. Del propio tenor de esta disposición se desprende que el Derecho nacional que autorice la adopción de una decisión individual automatizada debe establecer medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos del interesado⁹². Además, el tratamiento deberá respetar los requisitos establecidos en los arts. 5 y 6 RGPD⁹³.

Respecto a la tercera excepción, el consentimiento del interesado como base legitimadora para el tratamiento de datos personales es la clave de bóveda de la normativa de protección de datos. Sin embargo, no garantiza en absoluto un conocimiento y comprensión suficientes de las consecuencias

⁹⁰ Vid., art. 18 de la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios y art 29 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible. Sobre la obligación de los bancos de evaluar la solvencia del cliente antes de la concesión de un crédito, puede verse MARÍN LÓPEZ, M.J., «La obligación de evaluar la solvencia del prestatario en la Ley 5/2019, de contratos de crédito inmobiliario», *Revista de Derecho Patrimonial*, n. 50/2019, accesible en https://manueljesusmarin.es/wp-content/uploads/2022/02/doctrin_084.pdf.

⁹¹ Así lo explica el GT29 en sus *Directrices sobre decisiones individuales automatizadas*, cit., p.26.

⁹² El Considerando 71 RGPD establece que las medidas a adoptar deben incluir, en particular, la obligación del responsable del tratamiento de utilizar procedimientos matemáticos o estadísticos adecuados, de aplicar las medidas técnicas y organizativas apropiadas para garantizar que se reduzca al máximo el riesgo de error y se corrijan errores, y de asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, los efectos discriminatorios en las personas físicas.

⁹³ Como indica el TJUE, en su sentencia de 7 de diciembre de 2023, párrafos 65, 66 y 68, los Estados miembros no podrán adoptar normativas que autoricen las decisiones automatizadas o elaboración de perfiles incumpliendo los requisitos establecidos en los arts. 22.2.b) y 22.4 y en los arts. 5 y 6 RGPD. Para un mayor desarrollo de esta excepción puede verse PALMA ORTIGOSA, A., *op.cit.*, p. 9/25.

que implica la cesión y el tratamiento de dichos datos. Lo mismo ocurre con las decisiones automatizadas puesto que los interesados no son conscientes de la trascendencia e impacto de sus resultados ni de los posibles sesgos discriminatorios que pueden esconder. En cualquier caso, este consentimiento debe cumplir con los requisitos del art. 4.11 en relación con el Considerando 42 RGPD, es decir, debe ser informado, específico, inequívoco, libre y revocable⁹⁴.

Pues bien, en tales supuestos excepcionales, y más concretamente en los previstos en las letras a) y c), el precepto recoge una serie de garantías «mínimas» que deberá adoptar el responsable para salvaguardar los derechos e intereses legítimos del afectado por la decisión automatizada: concretamente, el *derecho a obtener intervención humana* por parte del responsable, a *expresar su punto de vista y a impugnar*⁹⁵ la decisión (art.22.3). A las que se debe añadir, tal como menciona el Considerando 71, la *información específica* al interesado. Las mismas garantías, al menos, deberá adoptar el Estado que autorice este tipo de decisiones en su ordenamiento en virtud del art. 22.2.b).

A continuación, se establecen dos importantes precisiones respecto a este tipo de decisiones que deben tenerse en consideración: por un lado, que la decisión automatizada no puede basarse en las categorías de datos especialmente protegidos por el art. 9.1 (art. 22.4); y por otro lado, que mediante Ley se podrá limitar el alcance de las obligaciones y derechos establecidos en el art. 22 en los numerosos supuestos del artículo 23 (art.23.1).

Respecto al tratamiento de las categorías especiales de datos (también conocidos como datos sensibles) vienen a coincidir prácticamente con las denominadas *categorías sospechosas* o *motivos protegidos* de la normativa antidiscriminatoria. Se trata, concretamente, de datos que revelen el origen étnico o racial, las opiniones políticas, religiosas o filosóficas, los datos genéticos o biomédicos y aquellos otros referentes a la vida u orientación sexual de la persona⁹⁶. Por tanto, cualquier sesgo en los resultados del sistema causado al tener en cuenta este tipo de datos de manera voluntaria o por error, supon-

⁹⁴ Analiza cada uno de estos requisitos, CASADESÚS RIPOLL, P., *La responsabilidad civil por el uso discriminatorio de los datos personales a través de la inteligencia artificial*, Granada, 2022, pp. 149-154.

⁹⁵ Sobre este concreto derecho, RIVAS VALLEJO, P. «Análisis...», *cit.*, p. 460 dice que «Tampoco se matiza si el derecho a impugnar la decisión tiene un marco de acción reducido a la interacción con “el responsable del tratamiento” o si tiene un contenido más amplio equivalente al derecho a reclamar contra la decisión empresarial, que debería entenderse en sentido interno, pues la legislación garantiza en todo caso el derecho a la reclamación administrativa o judicial (art. 24 CE)».

⁹⁶ Salvo en determinadas circunstancias mencionadas en el ap. 2, dispone el art. 9.1 que «Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométri-

dría el incumplimiento de este artículo cuando no concurra causa legítima para su tratamiento, además del incumplimiento de la prohibición legal de no discriminar.

Debe tenerse en cuenta que la prohibición de tratar categorías especiales de datos tiene excepciones. Así, cuando concurren una serie de circunstancias recogidas en el art. 9.2 su tratamiento estará permitido bajo ciertas condiciones. En concreto, se autoriza el tratamiento de datos sensibles *cuando sea necesario por razones de interés público esencial*, sobre la base del Derecho de la Unión o de los Estados miembros (letra g). Precisamente dicho fundamento ha sido el esgrimido en el RIA para justificar el tratamiento de estas categorías especiales de datos a través de sistemas IA. Evitar la discriminación que podría provocar el sesgo de los sistemas de IA se considera una cuestión de orden público esencial en virtud de la cual los proveedores deben ser capaces de tratar ese tipo de datos «*con carácter excepcional, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas*»⁹⁷ y *tras la aplicación de todas las condiciones aplicables establecidas en el presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680*»⁹⁸. Es el art. 10.5 el que se encarga de establecer las condiciones para que se pueda llevar a cabo dicho tratamiento.

B) *La prohibición general del art. 22 RGPD: presupuestos de aplicación a la luz de la última jurisprudencia del TJUE en su sentencia de 7 de diciembre de 2023*

Dos son los presupuestos que exige el art. 22.1 para que opere la prohibición que contiene: por un lado, que se trate de decisiones basadas *únicamente* en el tratamiento automatizado de datos personales; y por otro lado, que dichas decisiones tengan *efectos jurídicos o significativamente similares* en el interesado.

cos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física».

⁹⁷ En la Orientación General del Consejo sobre el RIA, de 25 de noviembre de 2022, el texto del art. 10.5 mencionaba como salvaguardias adecuadas para los derechos y libertades fundamentales, el establecimiento de «*limitaciones técnicas a la reutilización y la utilización de las medidas de seguridad y protección de la privacidad más recientes, tales como la seudonimización o el cifrado, cuando la anonimización pueda afectar significativamente al objetivo perseguido*».

⁹⁸ Vid., Considerando 70.

- a) Primer presupuesto: que se trate de una decisión exclusivamente automatizada

El primer presupuesto implica el uso de sistemas que de forma automática y sin intervención humana significativa adopten una decisión que afecte a la persona (por ejemplo, decidir qué candidatos para un puesto de trabajo se descartan en un proceso de selección y quiénes pasan a la fase de entrevista, rechazar automáticamente la concesión de un crédito o la concertación de un seguro, etc). Como se encargó de aclarar el GT29, para que se trate de decisiones exclusivamente automatizadas no debe haber una intervención humana responsable que analice la información procesada y cuente con poder o capacidad de modificar la decisión⁹⁹.

Surge la duda de si la prohibición se aplicaría a los casos en que esa intervención humana relevante se limitara a una o varias partes del proceso de decisión, pero no a todas. Podría defenderse que, en la medida en que dicha intervención humana significativa exista (aunque sea en una etapa del proceso), las decisiones no quedarían bajo el ámbito de aplicación del art. 22. Por tanto, en tales casos el afectado no gozaría de los derechos y garantías anteriormente comentadas. No obstante, creemos más acertado mantener que para poder eludir la aplicación del precepto, la existencia de intervención humana debería apreciarse en cada una de las decisiones parceladas dirigidas al mismo fin y no solamente en alguna parte del proceso. Así, por ejemplo, si un algoritmo selecciona las 10 mejores candidatas a un puesto de trabajo de entre las 1000 que se postulan, descartando automáticamente a las demás, existiría una decisión automatizada respecto de la que habría que garantizar los derechos recogidos en la norma, aunque las 10 últimas fueran evaluadas por una persona¹⁰⁰. Por el contrario, el art. 22 sería inaplicable si en ese proceso ha intervenido un supervisor que ha decidido quién pasa a la segunda fase y quién no, sobre la base de la recomendación que hace el sistema IA de apoyo a la decisión humana (y que, si lo considera oportuno, puede no seguir),

⁹⁹ *Directrices sobre decisiones individuales automatizadas*, cit., p. 23. Sobre lo que implica esta exigencia puede verse también RIVAS VALLEJO, P. «Análisis...», cit., p. 457 y ss.

¹⁰⁰ MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, *Información algorítmica en el ámbito laboral. Guía Práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral*, mayo 2022, p.10. Accesible en file:///C:/Users/ASUS/Downloads/algortca_laboral-1.pdf. Como explica RIVAS VALLEJO, P. «Análisis...», cit., p. 456, «la norma parece apuntar a un ámbito restringido del citado derecho a la explicabilidad, no extensible, por tanto, a decisiones automatizadas en parte del proceso de decisión, aun cuando esta parte sea especialmente relevante en el conjunto de factores que conducen a la decisión final». El problema de mantener esta interpretación, como sigue diciendo la autora, es que «si se considera que han sido presentados mil currículos, de los cuales han sido preseleccionados quince para su examen humano, el grueso del sesgo, donde probablemente radique la mayoría de discriminaciones por diversas causas protegidas, habrá quedado incluido en una fase íntegramente automatizada, sobre la cual no se ofrecerá explicación alguna».

salvo que esa intervención humana hubiera sido exclusivamente simbólica o ficticia, asumiendo sin más lo decidido por el sistema¹⁰¹.

En definitiva, para eludir tanto la prohibición como las obligaciones que impone el art. 22 a los responsables del tratamiento cuando hay base legitimadora del tratamiento automatizado, debe quedar claro que la intervención humana debe ser significativa en el sentido de ser realizada por una persona con competencia y autoridad sobre la decisión y que valore toda la información disponible, no siendo suficiente con que se limite a convalidar, replicar o reproducir acríticamente la decisión o recomendación del sistema. Su intervención no debe consistir en una mera supervisión superficial de los resultados del algoritmo sino en una participación real, relevante o sustancial en el proceso decisorio.

Del análisis de este primer presupuesto puede extraerse, como conclusión, que la regulación no afecta a todas las predicciones algorítmicas sino solo a aquellas que se integran en sistemas de decisión plenamente automatizados¹⁰². Por ello, y sobre la base de que en la práctica lo normal es que las decisiones no suelen tomarse de forma plena o puramente automática (sobre todo cuando son de una entidad considerable), sino como un elemento más de juicio, junto con otros, para tomar la decisión final, el art. 22 RGPD perdería cierta relevancia puesto que se aplica exclusivamente a una de las distintas formas de utilización de estos sistemas algorítmicos¹⁰³. Es decir, la prohibición que contiene gozaría de escasa aplicación en tanto en cuanto no abarca las decisiones semiautomatizadas y, en la actualidad, no es tan frecuente la toma de decisiones plenamente automatizadas que cumplan las condiciones que exige la norma. Lo más normal es que se utilicen los resultados de estos sistemas como elemento auxiliar que el operador humano puede tener en cuenta, o no, para adoptar su decisión final¹⁰⁴.

Dicha limitación supone una importante traba en la lucha contra la opacidad de los sistemas de IA (y por lo que a nosotros interesa, contra la discriminación algorítmica) por cuanto los sistemas que se usan como apoyo a la decisión también pueden arrojar resultados incorrectos y discriminatorios al

¹⁰¹ Como mantiene EGUÍLUZ CASTAÑEIRA, J.U., *op.cit.*, p. 344, si no se entendiera que esa intervención humana no ha de limitarse a reproducir la decisión del sistema, las empresas podrían eludir fácilmente la aplicación del art. 22, destinando un empleado a supervisar decisiones automatizadas, que en la práctica se limitara a asumir acríticamente sus resultados.

¹⁰² En este sentido, por todos, HUERGO LORA, A., «Una aproximación...», cit., p. 60 o GINÈS i FABRELLAS, A., *op.cit.*, p. 319. También se hace referencia a esta idea en MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, *Información algorítmica en el ámbito laboral...*, cit., p. 15, cuando se dice que la regulación europea usa un concepto restrictivo de algoritmo en la medida en que exige que tome decisiones íntegramente automatizadas.

¹⁰³ PALMA ORTIGOSA, A., *op.cit.*, p. 5/25.

¹⁰⁴ Por todos, HUERGO LORA, A., «Una aproximación...», cit., p. 71.

contener, por ejemplo, sesgos en el diseño o en los conjuntos de datos utilizados¹⁰⁵, y principalmente, por el denominado «sesgo de la automatización», es decir, la tendencia comprobada de que los humanos confiamos o creemos (erróneamente) que el resultado ofrecido por la máquina es mucho más acertado, objetivo y neutral que el nuestro, cuando ambos juicios no coinciden¹⁰⁶.

Por ello, en aras de una mejor defensa de los intereses del perjudicado por la decisión, señala el GT29 que, aunque la decisión automatizada o la elaboración de perfiles no cumplan la definición del art. 22.1, seguiría siendo aconsejable ofrecer la información ampliada o reforzada prevista en el RGPD¹⁰⁷. Ahora bien, a nuestro modo de ver, más allá de esta recomendación o consejo, lo que habría que plantearse sería la expresa ampliación del ámbito de aplicación de este derecho de información específico y demás garantías previstas en el precepto a los casos de decisiones semiautomatizadas, tal y como por ejemplo ha hecho nuestro legislador laboral en el art. 64.4 ET¹⁰⁸ y como parece sostener también el TJUE en su sentencia de 7 de diciembre de 2023 que será analizada *infra*.

b) Segundo presupuesto: efectos jurídicos o similares

Respecto al segundo presupuesto exigido por el art. 22 RGPD, esto es, que la decisión automatizada produzca *efectos jurídicos o significativamente simi-*

¹⁰⁵ GINÈS i FABRELLAS, A., *op.cit.*, p. 319

¹⁰⁶ En SOLAR CAYÓN, J.I., *op.cit.*, p. 170, se apunta que la literatura científica en sociología cognitiva y economía conductual muestra que es psicológicamente muy difícil desatender las recomendaciones de los sistemas algorítmicos, por lo que lo más probable es que las personas acaben siguiéndolas, especialmente, cuando se promueve el uso de estos sistemas bajo el argumento y con el objetivo de contribuir a erradicar la subjetividad y los errores humanos. Y BELTRÁN DE HEREDIA, I., «Automatización y obsolescencia humana», en *Retos jurídicos de la inteligencia artificial*, coord. por Agustí Cerrillo i Martínez y Miquel Peguera Poch, 2020, p. 120, manifiesta que se trata de un tipo de sesgo que, a pesar de estar presente en muchos ámbitos, supone un riesgo particular en aquellas personas que utilizan *software de apoyo para la toma de decisiones* en análisis y diagnóstico (por ejemplo, médicos, gestores de riesgo o analistas financieros).

¹⁰⁷ Vid., *Directrices sobre decisiones individuales automatizadas*, cit., p. 28.

¹⁰⁸ Esta reforma del ET fue realizada a través del Real Decreto-ley 9/2021, de 11 de mayo, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales, que fue convalidado posteriormente por la Ley 12/2021, de 28 de septiembre (conocida como *Ley rider*). Se modifica el art. 64.4 ET para incluir un derecho de información colectiva, que se suma al derecho de información individual previsto en el RGPD, y que se aplica aun cuando se trate de *sistemas semiautomatizados* de toma de decisión. En virtud de este derecho, la representación legal de la plantilla tendrá que ser informada de «los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que puedan incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles». Sobre este derecho señala GINÈS i FABRELLAS, A., *op.cit.*, p. 319 que, si bien se trata de una regulación pionera a nivel europeo que permite a la representación legal de la plantilla valorar la legalidad -e, incluso, potencial discriminatorio- de las variables utilizadas por el algoritmo, debería haberse acompañado con información estadística sobre el impacto del uso de dicha tecnología inteligente.

lares en las personas, se trataría de que la decisión afectara de alguna manera a los derechos o la esfera jurídica de la persona, como por ejemplo sucede cuando te deniegan un préstamo o una subvención pública, te excluyen de un proceso de selección laboral o te despiden de un trabajo¹⁰⁹. Es esencial, por tanto, que la decisión tenga el potencial de afectar significativamente a las circunstancias, al comportamiento o a las elecciones de las personas afectadas, impacte de forma prolongada o permanente en el interesado, o, en los casos más extremos, provoque la exclusión o discriminación de la persona¹¹⁰.

Algún autor pone en duda que esta clase de decisiones (que a veces ni siquiera se refieren a personas concretas, sino a grupos o a zonas) produzcan los «efectos jurídicos en el interesado» a que se refiere el precepto¹¹¹. Sin embargo, incluso en la conocida sentencia *Syri* del Tribunal de Distrito de La Haya, de 5 de febrero de 2020, se reconoce que los informes de riesgo elaborados por el sistema de IA acerca de la probabilidad de que determinados ciudadanos defraudaran al fisco, les afectaban «significativamente» de un modo similar a una decisión con efectos jurídicos.

A *sensu contrario*, las decisiones automatizadas basadas en datos personales que no tengan efectos o consecuencias jurídicas para los sujetos, no quedarían bajo el ámbito de aplicación del precepto analizado. Como ejemplo de este tipo de decisiones HERRERA DE LAS HERAS pone el de un restaurante que utiliza un sistema de reconocimiento facial y detección de emociones para determinar el grado de satisfacción del cliente¹¹². La decisión del sistema acerca del grado de satisfacción concreto de cada comensal no tendría efectos jurídicos para ellos en la medida en que no supondría que se les denegara el

¹⁰⁹ Pueden verse otros ejemplos de este tipo de decisiones en las *Directrices sobre decisiones individuales automatizadas*, cit., pp. 23-24. También en el Considerando 71 RGPD se pone como ejemplo la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Sin embargo, a pesar de dichos ejemplos, no resulta siempre evidente cuándo una decisión afecta significativamente a un sujeto. Como afirman MENDOZA, I./ BYGRAVE, L.A. «The Right Not to Be Subject to Automated Decisions Based on Profiling», *University of Oslo Faculty of Law Research Paper* n.20, 2017, p. 12, aunque puede deducirse que en aquellos casos en los que la decisión tenga impacto en la situación financiera o laboral del interesado estaremos ante un efecto significativo, el efecto concreto dependerá de las características de cada individuo, por lo que se deberá hacer un estudio *ad casum* sobre la significación o relevancia del efecto. Para EGUÍLUZ CASTANEIRA, J.U., *op.cit.*, pp. 342 y ss., un ejemplo de una decisión con «efectos jurídicos» sería una decisión judicial, o una decisión con respecto a un beneficio social otorgado por la ley, como el pago de la pensión. Por otro lado, un ejemplo de una decisión con efectos «significativamente similares» sería un banco que niega un crédito automáticamente. Y en base a lo que sostienen las Autoridades de Protección de Datos, la diferenciación de precios en línea podría «afectar significativamente de manera similar» a alguien, si conduce a «precios prohibitivamente altos que efectivamente excluyen a alguien de ciertos bienes o servicios».

¹¹⁰ SÁEZ LARA, C., *op.cit.*, p. 53.

¹¹¹ Así, HUERGO LORA, A., «Una aproximación...», cit., p. 61.

¹¹² HERRERA DE LAS HERAS, R., *op.cit.*, p. 655.

acceso en próximas visitas, o que se les cobrara más o menos en función de su grado de satisfacción, sino que simplemente iría dirigida a evaluar su grado de satisfacción. En su opinión, parece que en estos casos el cliente no podría negarse al escrutinio hecho por el sistema inteligente. No obstante, a nuestro modo de ver, si bien no tendría los derechos y garantías del art. 22.3 ni el derecho de información reforzado de los arts. 13.2.f), 14.2.g) y 15.1.h), sí tendría derecho a ser informado del resto de extremos que contemplan tales normas y gozaría del resto de derechos que otorga la normativa cuando se procede al tratamiento de datos personales (acceso, rectificación, oposición...).

Por el contrario, un ejemplo de decisiones automatizadas con efectos jurídicos en la persona podría ser el rechazo automático de una solicitud de préstamo bancario basado únicamente en el perfil crediticio del solicitante generado por un algoritmo. Este tipo de decisión sí que tendría un efecto o consecuencia jurídica directa sobre la persona porque afectaría a su capacidad para obtener un crédito y, potencialmente, a su situación financiera general.

Presentes los dos presupuestos anteriores serían aplicables las garantías del art. 22.3 RGPD así como la regulación específica en relación al derecho de información y acceso del interesado previsto en los arts. 13.2 f), 14.2 g) y 15.1 h)¹¹³, en cuya virtud, la persona afectada por la decisión tendrá *derecho a saber que está siendo objeto de una decisión automatizada*, es decir, derecho a conocer la existencia en sí del tratamiento automatizado de datos que le afectará, así como el derecho a que se le proporcione *información significativa sobre la lógica aplicada por el sistema y sobre la importancia y las consecuencias previstas de dicho tratamiento*. En consecuencia, los responsables estarían obligados a informar de ello (así como de su base legitimadora dada la prohibición general del art.22.1) y, al menos en tales casos, de los extremos anteriores. Por el contrario, no se aplicarían tales derechos y garantías si las decisiones no cumplieran los requisitos del art. 22, bien porque hubiera existido intervención humana significativa en su adopción (casos de decisiones semiautomatizadas), bien porque no desplegaran efectos jurídicos o similares sobre las personas.

Si bien esta conclusión era la que se venía manteniendo hasta el momento, la reciente sentencia del TJUE, de 7 de diciembre de 2023, ha sentado una interpretación distinta por lo que se refiere a los presupuestos del art. 22 RGPD, y en concreto, a su aplicación a las decisiones semiautomatizadas. Veámosla.

¹¹³ Como explican las *Directrices sobre decisiones individuales automatizadas*, cit., del GT29, p. 28, «ofrecer esta información también ayudará a los responsables del tratamiento a garantizar que cumplen algunas de las garantías obligatorias descritas en el artículo 22, apartado 3, y el considerando 71».

- c) La STJUE de 7 de diciembre de 2023, asunto C-634/21 (OQ y Land Hessen, con intervención de SCHUFA Holding AG)

En esta resolución el TJUE realiza una interpretación extensiva del art. 22 RGPD a fin de aplicar las garantías que contiene también a las decisiones parcial o semiautomatizadas¹¹⁴. El caso versaba sobre un litigio entre SCHUFA, una empresa alemana que proporciona información de solvencia a terceros, y OQ, un particular a quien un banco le denegó un préstamo en base a la información negativa que SCHUFA proporcionó sobre él. OQ ejerció su derecho de acceso a los datos registrados y su eliminación, pero SCHUFA se negó a revelar todos los datos utilizados en su evaluación. Solo cedió información genérica pero no los datos que tenía del afectado ni la ponderación de los mismos que había realizado en forma de valores de probabilidad. Justificó su negativa en que no había sido ella quien había denegado el crédito sino sus socios contractuales (es decir, el banco) e invocó también secretos comerciales¹¹⁵.

El Tribunal de lo Contencioso-Administrativo de Wiesbaden planteó dos cuestiones prejudiciales al Tribunal de Justicia sobre la interpretación del art. 6 y 22.1 RGPD, con el fin de determinar, por un lado, si la actividad realizada por SCHUFA (esto es, la generación automatizada de un valor de probabilidad transmitido a terceros que toman decisiones basadas en él) constituía una «decisión automatizada» en el sentido del art. 22 RGPD teniendo en cuenta que no era SCHUFA quien tomaba la decisión final; y por otro lado, si la negativa de SCHUFA a proporcionar información adicional al afectado suponía una vulneración de los derechos de protección de datos de OQ por estar obligada a ello, teniendo en cuenta que los terceros que tomaron la decisión final -en base a dicho valor de probabilidad- no disponían de tal información.

¹¹⁴ Sobre esta resolución puede verse, COTINO HUESO, L., «La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial» Diario LA LEY, N° 80, Sección Ciberderecho, 17 de Enero de 2024. Recuperado de La Ley Digital, LA LEY 1301/2024. Para este autor «es reconfortante observar un progresivo reconocimiento normativo de la importancia de las garantías en decisiones parcial o semi-automatizadas», teniendo en cuenta que tanto la Carta de Derechos Digitales en España, como algunas legislaciones de protección de datos fuera de la UE también las recogen expresamente, como por ejemplo, la de Ecuador. También en Canadá o EEUU la definición de sistema de decisiones automatizado (*automated decision system*) incluye tanto las decisiones totalmente automatizadas como las de apoyo a la decisión. Vid., por ejemplo, el proyecto de Ley de Responsabilidad Algorítmica de 2022 de EEUU (sección 2; Definiciones).

¹¹⁵ Las entidades de información y análisis de riesgo (como SCHUFA o en el caso del mercado español, Equifax o Experian) analizan el riesgo de un prestatario, combinando factores objetivos y subjetivos a partir de la información de que disponen sobre el prestatario, y/o de la información que sus socios comerciales (por ejemplo, los bancos) les proporcionan con el fin de que calculen esa puntuación o valor de probabilidad determinado. No obstante, son dichos socios comerciales los que toman la decisión final sobre la ejecución (o modo de ejecución) de un contrato con el prestatario, es decir, los que deciden la concesión o denegación del crédito, si bien con base en dicho valor.

En su sentencia, el Tribunal se detiene en el análisis de los presupuestos de aplicación del art. 22, que concreta en tres: en primer lugar, la existencia de una «decisión»; en segundo lugar, la necesidad de que ésta se base «únicamente» en un tratamiento automatizado de datos personales (incluida la elaboración de perfiles); y en tercer lugar, que la decisión despliegue «efectos jurídicos» en el interesado o le «afecte significativamente de modo similar».

Respecto al concepto de «decisión» al que se refiere el art. 22.1 RGPD, sostiene una interpretación extensiva en la línea mantenida por el Abogado General en el punto 38 de sus conclusiones. Entiende que puede incluir diversos actos con potencial para afectar al interesado de múltiples maneras y que engloba el resultado del cálculo de la solvencia de una persona en forma de un valor de probabilidad relativo a su capacidad para hacer frente a sus compromisos de pago en el futuro (párrafo 46).

Por lo que respecta al requisito de que la decisión deba estar «basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles», mantiene, como señalaba también el Abogado General en el punto 33 de sus conclusiones, que no se discute que una actividad como la que realiza SCHUFA responde a la definición de «elaboración de perfiles» del art.4.4 RGPD y, por tanto, que en el presente asunto se cumple este requisito, habida cuenta de que el tenor de la primera cuestión prejudicial se refiere expresamente a la generación automatizada de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de su capacidad para satisfacer un préstamo en el futuro (párrafo 47).

Por último, respecto al requisito de que la decisión deba producir «efectos jurídicos» en el interesado o «[afectarlo] significativamente de modo similar», sostiene que del propio tenor de la primera cuestión prejudicial se desprende que la acción del tercero al que se transmite el valor de probabilidad (el banco) está basada «de un modo determinante» en dicho valor. Así pues, según las apreciaciones de hecho del órgano jurisdiccional remitente, en el caso de que un consumidor solicite un préstamo a un banco, un valor de probabilidad insuficiente dará lugar a que el banco deniegue la concesión del préstamo solicitado en la práctica totalidad de los casos (párrafo 48). En estas circunstancias, considera que la decisión sobre el valor de probabilidad, cuanto menos, afecta al interesado significativamente (párrafo 49) ¹¹⁶.

¹¹⁶ Sobre las dificultades prácticas que pueden derivarse de la consideración de un valor como «determinante» o «no determinante», pueden verse las consideraciones de NEGRO, A., Y SANCHEZ, A., «El veredicto del TJUE sobre el *credit scoring*», accesible en <https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/veredicto-tjue-sobre-credit-scoring>. Observan, entre otras cosas, que aunque el TJUE nada indica al respecto, cabe entender que la calificación de un valor como «determinante» no depende de que sea el único valor o puntuación que se tenga en cuenta para

Por tanto, el TJUE entiende que la generación automatizada del valor de probabilidad proporcionado por SCHUFA y utilizado por el banco para tomar decisiones sobre créditos, debe ser calificada como una decisión individual automatizada (basada en una elaboración de un perfil) que afecta significativamente al interesado. Ello implica la necesidad de cumplir con las disposiciones del RGPD sobre protección de datos y determina la obligación de SCHUFA de divulgar información adicional al interesado¹¹⁷.

Esta interpretación se ve corroborada por el contexto en el que se inscribe el art. 22.1 RGPD, así como por los objetivos y la finalidad que persigue dicho Reglamento. Según entiende el TJUE, de no mantener esta interpretación existiría una laguna jurídica que mermaría la aplicación, finalidad y protección que se pretende con el art. 22 RGPD. Una interpretación restrictiva del precepto que excluyese decisiones como la controvertida (esto es, la generación automatizada de un valor de probabilidad) por considerarlas un mero *acto preparatorio* ejecutado por una agencia comercial, calificando únicamente como «decisión» del art. 22 el acto final adoptado por la tercera entidad, generaría un riesgo de elusión del precepto ya que los interesados no podrían ejercitar sus derechos frente a la empresa que calculó su probabilidad de impago, ni siquiera cuando (como ocurrió en este caso) el tercero que hubiera adoptado la decisión final no tuviera toda la información relevante acerca del tratamiento de datos realizado sobre interesado, al haber recibido, únicamente, el valor de probabilidad solicitado¹¹⁸.

En definitiva, como explica COTINO HUESO, para el TJUE las garantías del art. 22 RGPD también se pueden aplicar a los actos, hechos o datos sobre los que se sustentan las decisiones automatizadas, como los perfiles o ponderaciones automatizados que han estado en la base de la decisión finalmente adoptada¹¹⁹. Ello a pesar de que *formalmente* la decisión final se adopte por

la toma de las decisiones pertinentes, *sino de que del valor trasladado haya dependido la decisión final* (la cursiva es nuestra).

¹¹⁷ Esta conclusión la recoge el párrafo 73 en los términos siguientes: el art.22.1 del RGPD «debe interpretarse en el sentido de que la generación automatizada, por una agencia de información comercial, de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de la capacidad de esta para hacer frente a compromisos de pago en el futuro constituye una “decisión individual automatizada”, en el sentido de la mencionada disposición, cuando de ese valor de probabilidad dependa de manera determinante que un tercero, al que se comunica dicho valor, establezca, ejecute o ponga fin a una relación contractual con esa persona».

¹¹⁸ Vid., párrafos 61 y 63.

¹¹⁹ Ello supone, por un lado, que el responsable del tratamiento está sujeto a obligaciones adicionales de información en virtud de los artículos 13, apartado 2, letra f), y 14, apartado 2, letra g), de dicho Reglamento; y por otro lado, que el interesado tiene derecho, en virtud del artículo 15, apartado 1, letra h), del mencionado Reglamento, a obtener del responsable del tratamiento, en particular, «información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado» (párrafo 56). Estos requisitos más estrictos para la

una entidad distinta a la que hace el perfilado o ponderación previa, o de que haya aparentemente una intervención humana. Por ende, esta sentencia expande el alcance del art. 22 RGPD más allá del responsable formal de la decisión, para abarcar a aquellos que procesen datos y que efectúan *materialmente* el tratamiento automatizado para el responsable bajo otras posiciones jurídicas, como la de encargado por cuenta de quien finalmente toma la decisión¹²⁰.

Concluimos, junto al autor citado, que el criterio garantista que adopta el TJUE en esta resolución respecto de las decisiones automatizadas sienta un precedente que podrá proyectarse en muchos otros supuestos en el futuro. Precedente que, además, a nuestro juicio era totalmente necesario para subsanar el insuficiente ámbito de aplicación del art.22, teniendo en cuenta que, al menos en la práctica actual, es mucho más frecuente tomar decisiones con apoyo en los resultados de un sistema de IA, que delegar plenamente en ellos las decisiones finales¹²¹.

licitud de una toma de decisiones automatizada, así como las obligaciones adicionales de información del responsable del tratamiento y los derechos de acceso adicionales del interesado correspondientes se explican por la finalidad que persigue el artículo 22 del RGPD, que consiste en proteger a las personas contra los riesgos específicos para sus derechos y libertades que supone el tratamiento automatizado de datos personales, incluida la elaboración de perfiles (párrafo 57).

¹²⁰ COTINO HUESO, L., «La primera sentencia del Tribunal de Justicia de la Unión Europea...», cit., se refiere a los sujetos intervinientes como «responsable formal de la decisión» (en este caso el Banco) y «tercero encargado del tratamiento de datos» (en este caso, Schufa) y considera que, en base a este pronunciamiento, las «garantías del artículo 22 RGPD se proyectan y van más allá del responsable -al menos formal- que toma la decisión respecto del afectado, generando obligaciones a un tercero encargado que ha tratado datos del afectado». No obstante, para otros autores, las agencias como Schufa que prestan servicios de *credit scoring* actuarán directamente en calidad de «responsables del tratamiento» cuando concurran los tres requisitos analizados por el TJUE y precisamente por ello deberán cumplir las obligaciones que el RGPD impone a los mismos: por un lado, asegurar la aplicación de alguna de las excepciones previstas en el artículo 22.2 y contar con una base legitimadora el tratamiento de los datos de los prestatarios que deberán probar. Asimismo, deberán garantizar el cumplimiento de la normativa aplicable (por ejemplo, aplicando las medidas técnicas y organizativas apropiadas para la seguridad de la información y la reducción del riesgo de error al máximo o garantizar los derechos de los interesados). Así lo mantienen NEGRO, A., Y SANCHEZ, A., *op.cit.loc.cit.* Sea como fuere, en ambos casos los autores coinciden en que los sujetos que *materialmente* efectúan el tratamiento automatizado, perfilado o ponderación de datos quedarían sujetos a ciertas obligaciones.

¹²¹ No obstante, como augura la doctrina, esta situación parece que se revertirá en un futuro no muy lejano. En este sentido, afirma PALMA ORTIGOSA, A., *op.cit.*, p. 6/25, que «el paso del tiempo hará que las decisiones automatizadas que ahora suelen utilizarse como un parámetro más de apoyo a la hora de tomar una decisión determinada, se conviertan en la regla a seguir, pudiendo llegar un momento de estandarización donde se pase de la desconfianza de la máquina, al recelo de la decisión que pueda adoptar un humano contraria a la que ha indicado el algoritmo, de manera que ya no se dude de la máquina sino de la persona».

4.2.2. Contenido del derecho de información de los arts. 13.2 g), 14.2 g) y 15.1 h)

El RGPD no concreta qué implica el deber de proporcionar «información significativa sobre la lógica aplicada» y si dicha expresión conlleva o no el derecho a conocer el código fuente del algoritmo y su funcionamiento. Dicha omisión ha hecho que surjan dudas y vacilaciones acerca de esta cuestión¹²². Es opinión ampliamente compartida que esa disposición del RGPD no impone una obligación de informar y dar acceso de forma exhaustiva al código fuente del algoritmo utilizado para adoptar la decisión, lo que, por otra parte, tampoco sería de utilidad en muchos casos para el interesado si no se comparten también los conjuntos de datos utilizados, por cuanto que en los sistemas adaptativos el código fuente va cambiando¹²³. Según las *Directrices sobre deci-*

¹²² Sobre este asunto planteaba RUBI PUIG dos posibilidades: que la información a suministrar tuviera que consistir en una explicación general del modelo (*model-based explanation*) o en explicar cómo se adoptó una decisión basada en los datos particulares del afectado (*subject-based explanation*). Vid., «Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores», *Revista De Educación Y Derecho*, 24, 2021, <https://doi.org/10.1344/REYD2021.24.36304>, p. 17/24. Sobre esta doble posibilidad, aclara MEDINA GUERRERO, M., *op.cit.*, p. 161, que el hecho de que la información deba facilitarse al recabarse los datos o en un plazo breve de tiempo después (ex arts. 13.2 y 14.3a) hace que en esta fase (previa a la toma de decisión) la obligación de informar no pueda traducirse en la exigencia de asegurar la explicabilidad, ni la fundamentación de una decisión en particular. Lo que debe ponerse en conocimiento del interesado es la descripción de los tipos de datos y los factores que toma en consideración el sistema, las categorías del árbol de decisión y la ponderación de tales factores a nivel global (la cursiva es nuestra). Con esa información el afectado debe poder prever qué papel juegan (o pueden jugar) sus diferentes datos objeto de tratamiento en la formación de la decisión a tomar, así como estar en condiciones de acomodar su conducta a los criterios que resultan determinantes para adoptar la decisión. Para NAVAS NAVARRO, S., «La perspectiva de género...», *cit.*, se puede interpretar que la lógica de la que se debe informar en estos casos es la lógica computacional empleada y se trataría de que se pudiera conocer, en la medida de lo posible, el proceso de toma de decisiones para ver si existe algún sesgo o error en el procesamiento de los datos.

¹²³ Según concluye el GT29 en sus *Directrices sobre decisiones individuales automatizadas*, p. 28, dicho deber de proporcionar información no consiste en revelar todo el algoritmo y menos aún su código fuente, o el secreto empresarial que lo protege. A la misma conclusión llega, por ejemplo, el MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, *Información algorítmica en el ámbito laboral. cit.*, pp. 12-15, según el cual, «la obligación de información derivada de los artículos 13.2.f) y 14.2.g) 15.1.h) RGPD y 64.4.d) ET no puede interpretarse como la obligación empresarial de facilitar el código fuente del algoritmo». Comparten esta postura, RIVAS VALLEJO, P., «Herramientas desde el derecho antidiscriminatorio...», *cit.*, p. 552; NÚÑEZ SEOANE, J., *op.cit.*, p. 307, o LAZCOZ MORATINOS, G., *op.cit.*, entre otros. Para la mayoría de la doctrina, este derecho de información no implica el derecho a acceder al algoritmo, no solo porque puede estar protegido por secreto empresarial, sino porque implicaría acceder a centenares de páginas de códigos indescifrables. Por el contrario, como precisa GINÉS i FABRELLAS, A., *op.cit.*, p. 319, implica el derecho a obtener información sobre las variables o métricas utilizadas por el algoritmo para la elaboración de perfiles o toma de decisiones automatizada, su ponderación en la ecuación final y las consecuencias que pueden derivarse para la persona. Como explica PALMA ORTIGOSA, A., *op.cit.*, p.14/25, el responsable del tratamiento debe explicar, en la medida de lo posible, el funcionamiento del programa informático, aportando información útil para el interesa-

siones individuales automatizadas del GT29, se trataría de ofrecer información conforme al *principio de transparencia* en términos sencillos y comprensibles, pero suficientemente exhaustiva para que el interesado pudiera entender *los motivos de la decisión*, sin necesidad de incluir una explicación compleja sobre los algoritmos utilizados, lo que podría ser opaco, confuso, e incluso conducir a la fatiga informativa¹²⁴. A nuestro modo de ver, el *quid* de la cuestión sería que la información proporcionada permitiera al interesado hacer efectivos los derechos de los que es titular. Por tanto, creemos junto con un sector doctrinal, que dicha información no sería suficiente ni significativa si impediera al interesado ejercitar los derechos y garantías que el propio art. 22 RGPD le otorga, esto es, oposición, revisión, alegación e impugnación de la decisión¹²⁵.

Sobre el contenido concreto de este derecho es interesante la opinión del Abogado General Priit Pikamäe en el asunto C-634/21 y en los asuntos acumulados C-26/22 y C-64/22 SCHUFA Holding y otros, al que hicimos referencia en el apartado anterior. Considera que *no es suficiente con dar una explicación genérica sobre cómo funciona el proceso de toma de decisión, sin indicar los datos específicos que se tienen de la persona y que han sido tenidos en cuenta para elaborar el informe negativo de solvencia*. A su juicio, «la obligación de proporcionar “información significativa sobre la lógica aplicada” debe entenderse en el sentido de que incluye *explicaciones suficientemente* detalladas sobre el método utilizado para el cálculo del *score* y sobre las *razones que han conducido a un resultado determinado*. En general, el responsable del tratamiento debería proporcionar al interesado información general, en particular sobre los *factores que han sido tenidos en cuenta en el proceso de toma de decisiones y sobre su importancia relativa desde el punto de vista agregado, que también le resulte útil para impugnar cualquier “decisión” en el sentido de la disposición del RGPD* que consagra el “derecho” a no ser objeto de

do - como por ejemplo los factores que más han influido en la elaboración del perfil - que le permita comprender el proceso y pueda así ejercer el resto de los derechos que le reconoce el RGPD en su artículo 22.3. En la *Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo*, sobre la mejora de la aplicación y modernización de las normas de protección de los consumidores de la Unión, también se aclara que no debe exigirse a los comerciantes que revelen el funcionamiento detallado de sus mecanismos de clasificación (incluidos los algoritmos), sino sólo una descripción general de los principales parámetros que determinan la clasificación, si bien no es necesario que dicha descripción se presente de un modo personalizado para cada una de las consultas concretas efectuadas (vid., Considerandos 22 y 23).

¹²⁴ La AEPD señala que según la RAE la palabra «*significativa*» denota «*Que da a entender o conocer con precisión algo*» y esto habría que interpretarlo como información que, proporcionada al interesado, le hace consciente del tipo de tratamiento que se está llevando a cabo con sus datos y que le proporciona certeza y confianza sobre sus resultados, lo que está relacionado con el concepto de «*explicabilidad*» del tratamiento mediante IA.

¹²⁵ En este sentido, por ejemplo, NÚÑEZ SEOANE, J., *op.cit.*, p. 307 y NAVAS NAVARRO, S., «La perspectiva de género...», *cit.*, p. 15/23.

una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles»¹²⁶.

Sin perder de vista las premisas y consideraciones anteriores, habría que aclarar sobre qué extremos concretos se debería informar al interesado. Tal como indica la AEPD, aunque la respuesta dependerá del tipo de componente de IA utilizado, un ejemplo de información que podría tener relevancia para el interesado podría ser la siguiente: *«El detalle de los datos empleados para la toma de decisión, más allá de la categoría, y en particular información sobre los plazos de uso de los datos (su antigüedad); la importancia relativa que cada uno de ellos tiene en la toma de decisión; la calidad de los datos de entrenamiento y el tipo de patrones utilizados; los perfilados realizados y sus implicaciones; los valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia; la existencia o no de supervisión humana cualificada; la referencia a auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada; en el caso de que el sistema IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo»*¹²⁷.

Por su parte, el Ministerio de Trabajo y Seguridad Social de España publicó en 2022 una *Guía práctica sobre la obligación de los empresarios de informar a los trabajadores sobre el uso de algoritmos*¹²⁸ que, aunque dirigida al ámbito de las relaciones laborales, creemos extrapolable a cualquier otro, al menos en lo relativo al contenido concreto de la información que deberá proporcionarse al interesado respecto del sistema algorítmico utilizado para la toma de decisiones que le afectan. En dicho documento se establece, con gran detalle, que deberá informarse de los siguientes extremos:

- a) *Información sobre el uso de algoritmos o sistemas de IA* para tomar decisiones automatizadas, incluyendo la elaboración de perfiles, identificando la tecnología utilizada por parte del algoritmo y las decisiones respecto de las que se utiliza tal tecnología. Esto incluiría, por ejemplo, informar sobre si la tecnología empleada genera un algoritmo de «caja negra» o si se trata de un algoritmo de aprendizaje continuo, el concreto *software* o producto utilizado y si cuenta, en su caso, con algún tipo de certificación, la empresa suministradora, si la em-

¹²⁶ Comunicado de prensa del TJUE n. 49/2023, 16 de marzo de 2023, con las conclusiones del Abogado General disponible en: https://curia.europa.eu/jcms/jcms/Jo2_7052/es/?annee=2023. Las cursivas del texto son nuestras.

¹²⁷ P. 24/53.

¹²⁸ Dicha Guía, que fue elaborada por una comisión formada por expertos en algoritmos, concreta y sistematiza las obligaciones empresariales de información con el fin de garantizar, entre otros, el derecho fundamental a la no discriminación.

presa ha realizado alguna alteración sobre el producto, o el grado de intervención humana cualificada en las decisiones adoptadas, esto es, si las mismas se adoptarán mediante sistemas de IA o simplemente con apoyo en los resultados de dichos sistemas.

- b) *Información significativa, clara y simple sobre la lógica y funcionamiento del algoritmo*, que incluiría tanto *las variables tomadas en consideración* (entendidas como la información o factores utilizados por el algoritmo para tomar la decisión o la elaboración del perfil¹²⁹, incluyendo si algunas de estas variables son datos personales), como *los parámetros utilizados* (entendidos como la ponderación relativa de cada variable en el modelo para la toma de la decisión, así como cualquier cambio de estos parámetros que modifique el comportamiento del algoritmo)¹³⁰. También habría que informar sobre las *reglas e instrucciones utilizadas por el algoritmo*, entendidas como las reglas programación (ya sea las programadas de forma expresa o las derivadas del aprendizaje del algoritmo) que conducen a la toma de la decisión¹³¹ y sobre los *datos de entrenamiento* y, en su caso, *validación* (ya que estos también influyen en su lógica o instrucciones del algoritmo), su calidad (adecuación, pertinencia, minimización atendiendo a la finalidad para los que fueron obtenidos, etc.) y el *tipo de patrones identificados en los datos de entrenamiento*¹³². En casos de elaboración de perfiles, las métricas de precisión o error en las tareas automatizadas (clasifica-

¹²⁹ En caso de elaboración de perfiles, también hay que informar de la tipología de perfiles que elabora el algoritmo y, específicamente a la persona trabajadora ex artículos 13.2.f) y 14.2.g) RGPD, habría que darle *información sobre la asignación concreta a uno de ellos*.

¹³⁰ Por ejemplo, en un sistema algorítmico utilizado en un proceso de selección, las variables podrían ser la formación de la persona o la experiencia profesional previa, y los parámetros serían el peso relativo que tiene cada variable en la decisión final de selección o contratación (v.gr. el modelo podría ordenar a las personas en atención a su experiencia profesional previa -valorada en un 40%- , formación -valorada en un 20%-etc., hasta alcanzar el 100%).

¹³¹ En un sistema IA utilizado por una plataforma de reparto de comida a domicilio, las reglas e instrucciones podrían ser que la asignación de pedidos entre sus repartidores se realizara de la siguiente manera: (i) excluyendo a las personas que se encuentran a una distancia superior de 1 km del restaurante, (ii) puntuando en una escala de X a Y en un 50% a las personas que se encuentran a una distancia mínima de 1 km del restaurante y en otro 50% a las personas con una disponibilidad mínima de 10 horas en alta demanda en las últimas dos semanas y (iii) asignando el pedido a la persona que obtuviera una puntuación superior; así como las demás reglas de programación, tales como aplicar las anteriores instrucciones a las personas conectadas en ese momento, excluir a las personas que están en un pedido en curso, etc.

¹³² Por ejemplo, en un algoritmo para un proceso de selección la empresa tendría que comunicar que ha utilizado (i) los datos de la plantilla de la empresa de los últimos 10 años; (ii) obtenidos cumpliendo con las exigencias de protección de datos, específicamente la obligación de haber informado a estas personas que sus datos serían reutilizados para el entrenamiento de un algoritmo para elaborar perfiles; y (iii) informar que, analizando los datos de entrenamiento, ha identificado el patrón estadístico que, por ejemplo, las personas con una formación en A cumplen un X% mejor

ción, puntuación, regresión, ordenación...) de las personas en los distintos perfiles. Y, por último, la referencia a las *auditorías* realizadas (en el caso de sistemas adaptativos o evolutivos la última auditoría realizada) *especialmente sobre las posibles desviaciones de los resultados de las inferencias*, o la *evaluación de impacto* realizada por parte de la empresa o una tercera empresa respecto del algoritmo o sistema de decisión automatizada utilizado.

- c) Información sobre las *consecuencias que puede tener sobre la persona la decisión* adoptada (por ejemplo, obtener un puesto de empleo o determinar las concretas condiciones laborales)¹³³.

En los casos en que las decisiones automatizadas exigieran la previa realización de una evaluación de impacto (art. 35 RGPD), el contenido de la información suministrada podría ser aún más exhaustivo, ya que sería ésta la que determinaría las «medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado»¹³⁴.

Toda la información suministrada debería de cumplir, además, las exigencias formales y el nivel de transparencia del art. 12 RGPD, esto es, habría de facilitarse de forma clara, simple y comprensible a fin de que el interesado pudiera ejercer sus derechos.

Para garantizar la efectividad de dichos derechos, el RGPD confiere poderes de investigación y sanción a la autoridad de control (vid., arts. 53 y 83). Para un sector de la doctrina, esta correlación de derechos individuales y de

sus funciones para un puesto determinado, en comparación con aquellas personas que tienen una formación en B.

¹³³ Además, en el ámbito laboral, debe informarse a los representantes de los trabajadores sobre el impacto que las decisiones adoptadas mediante algoritmos o sistemas de decisión automatizada tienen en materia de igualdad y no discriminación entre mujeres y hombres. Así se deriva del artículo 64.3 ET que reconoce el derecho de la representación legal de la plantilla de acceder a información referente a la aplicación en la empresa del derecho a la igualdad y no discriminación entre mujeres y hombres. Así como del artículo 7 Real Decreto 901/2020, referente al diagnóstico en un contexto de elaboración de un Plan de Igualdad.

Vid., AEPD., *Adecuación...*, cit., pp. 24 y ss., en relación con el alcance de la información sobre la «importancia» y «consecuencias previstas» apunta que la misma debe versar «sobre el tratamiento previsto o futuro, y sobre cómo puede afectar la decisión automatizada al interesado».

¹³⁴ Para NÚÑEZ SEOANE, J., *op.cit.*, pp. 312-313, la evaluación de impacto es un recurso alternativo para que el responsable del tratamiento que por legítimos motivos no quiera o no pueda revelar el funcionamiento del algoritmo, pueda justificar y demostrar ante el interesado con plenas garantías que las decisiones automatizadas que adopte no supondrán un riesgo para sus derechos y libertades. Para RIVAS VALLEJO, P., «Herramientas desde el derecho antidiscriminatorio...», cit., p. 553, a diferencia de las auditorías del algoritmo, la evaluación de impacto permite actuar igualmente con carácter previo a la implantación de decisiones normativas o privadas que comporten el uso de algoritmos de decisión con el fin de evitar su impacto futuro y constituiría una barrera adicional a la auditoría de la IA y a la participación de la representación legal de los trabajadores ex art. 65.5 ET.

poderes o competencias de la AEPD es lo que realmente garantiza el cumplimiento de los deberes de *transparencia hacia el interesado*, y por ende, la efectividad del derecho a una explicación de las personas afectadas por las decisiones automatizadas¹³⁵.

Llegados a este punto, y en base a todos estos mimbres, se puede concluir que el RGPD se erige en uno de los principales instrumentos para hacer frente a la opacidad de los sistemas de toma de decisiones con impacto en las personas. Por un lado, porque trata de impedir el *primer nivel de opacidad* al que nos referíamos *supra* cuando establece en los arts.13.2 f), 14.2 g) y 15.1 h) el derecho a ser informado de la *existencia de decisiones automatizadas*¹³⁶. Así, los interesados no deberían ignorar, en teoría, que el proceso decisorio que les afecta se va a realizar por medio de un tratamiento automatizado de sus datos personales. El problema reside en que, en la práctica, no llegan a ser conscientes de ello porque los responsables del tratamiento no les informan de este extremo al considerar que su decisión no es automatizada, aunque de hecho sí lo sea¹³⁷. Por otro lado, porque pretende evitar el *segundo nivel de opacidad*, ya que en tales casos deberá proporcionarse al interesado información significativa con el contenido y alcance anteriormente comentados. Por ende, puede afirmarse que en cierta medida dicha normativa contribuye a que el interesado pueda desafiar la validez de un algoritmo y pueda acceder a la ponderación que se le otorga a sus diversos elementos y a cualquier conclusión errónea a la que llegue.

Sin perjuicio de lo afirmado, la efectividad del derecho de información reconocido en el RGPD y su correlativo deber de transparencia, ha sido puesta en duda por la doctrina en los casos en que se emplean sistemas automatizados de decisiones basados en técnicas de IA como el *machine o deep learning*. Ello por diversas razones: por un lado, porque cuando se trata de algoritmos de *aprendizaje automático* que van modificándose progresivamente y de forma autónoma, es difícil proporcionar la información sobre la lógica del algoritmo por el efecto de caja negra que los caracteriza; por otro lado, porque como se explicó en su momento, en muchos casos se alegan derechos de propie-

¹³⁵ En este sentido, SÁEZ LARA, C., *op.cit.*, pp. 52 y ss.

¹³⁶ LAZCOZ MORATINOS, G., *op.cit.*, p. 293.

¹³⁷ Advierte de este hándicap PALMA ORTIGOSA, A., *op.cit.*, p. 4/25, para quien, la indeterminación de los conceptos jurídicos recogidos en el art. 22 RGPD, conlleva que en muchas ocasiones los responsables desconocerán de buena voluntad si se trata de un tratamiento al que deban aplicarse las reglas del precepto. Además, teniendo en cuenta que este precepto establece mayores exigencias para ellos y más derechos en favor de los titulares de los datos, ante situaciones dudosas tenderán a huir de su aplicación por entender que el tratamiento que están llevando a cabo no se asimila al definido en el precepto. Esclarecer todos estos conceptos jurídicos ayudaría al conjunto de operadores jurídicos a determinar cuándo el tratamiento concreto que se está llevando a cabo se subsume en el art.22 y cuándo no.

dad intelectual o secreto empresarial para no ofrecer información algorítmica a los interesados, no habiendo una postura doctrinal unánime acerca de la prevalencia o no de dichos derechos sobre los derechos o intereses de los individuos afectados por el tratamiento de sus datos personales cuando ambos entran en conflicto¹³⁸. Estas y otras razones llevan a un sector doctrinal a mantener que si bien el art. 22 RGPD es útil en el contexto de la protección de datos, no lo es tanto para el control del uso de la IA aplicada a datos masivos¹³⁹.

No obstante, a nuestro modo de ver, en la medida en que hay consenso en que sería suficiente con compartir una explicación funcional en lenguaje común para que cualquier persona interesada, sin los conocimientos técnicos suficientes, pudiera entender bajo qué parámetros ha podido ser afectado por un modelo matemático de decisión, sin necesidad de revelar el código fuente o el secreto empresarial que lo protege, se evitarían en gran medida perjuicios a los derechos de propiedad intelectual o secretos comerciales y la negativa a proporcionar información carecería de justificación. Más aún si se tiene en cuenta que los expertos mantienen que existen métodos en la ciencia de la computación que permiten supervisar el modelo para averiguar si es necesario hacer ajustes o correcciones que no comprometen el contenido del algoritmo cuando está sujeto a derechos de propiedad intelectual o incluso por razones de seguridad¹⁴⁰.

4.3. LA TRANSPARENCIA Y LA EXPLICABILIDAD EN EL REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 13 DE JUNIO DE 2024 POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL

La transparencia ocupa un lugar destacado en el RIA y se refiere tanto al grado de implantación en un sistema (finalidad, diseño, función y datos)

¹³⁸ Sobre esta polémica puede verse LÓPEZ-TARRUELLA MARTÍNEZ, A., *op.cit.*, pp. 197-199.

¹³⁹ Así lo entiende REBOLLO DELGADO, L., *op.cit.*, pp. 108, para quien «dicho precepto aporta una solución tangencial a un problema sobrevenido, como es la aplicación de la IA a bases masivas de datos, por lo que su eficacia es limitada. Parece necesaria una regulación más específica, que concrete todas las posibilidades y lo haga desde la perspectiva de la protección del usuario, de la persona implicada. Pero aquí nos volvemos a encontrar con el problema recurrente de qué tipo de información ofrecemos, qué nivel técnico tiene, y en qué grado es entendible para el usuario o titular de los datos. Este problema de aplicabilidad no es menor, y plantea la vuelta a la dinámica de la Directiva 95/46/UE y que desterró el RGPD, es decir, que al responsable o encargado del tratamiento no le es suficiente con cumplir la norma, sino que debe conseguir la finalidad propuesta por ella. Esto supone un endoso al responsable o encargado del tratamiento de la teleología del mandato jurídico de la norma, cuya efectividad suele quedar difuminada».

¹⁴⁰ RIVAS VALLEJO, P., «Herramientas desde el derecho antidiscriminatorio...», *cit.*, p. 555, citando estudios sobre el tema.

como al modo en que se utiliza y a las repercusiones que genera¹⁴¹. Además, aunque el RIA aboga principalmente por la *transparencia interna* (sobre todo hacia los responsables del despliegue), también establece algunas obligaciones a favor de la *transparencia externa* y ha acabado incorporando, como novedad destacable respecto a su versión inicial, el derecho a una explicación de las personas afectadas por las decisiones algorítmicas.

4.3.1. Obligaciones de transparencia y comunicación de información

A) Sistemas de alto riesgo

Cuando los sistemas no son lo suficientemente transparentes y explicables, ni están bien documentados, pueden impedir el ejercicio de derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, el derecho de defensa y la presunción de inocencia¹⁴². Para evitar la conculcación de tales derechos, el RIA establece, en su art. 13.1, que los sistemas de alto riesgo «se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones oportunas previstas en la sección 3». De esta disposición pueden extraerse varias ideas:

En primer lugar, en cuanto al *grado de transparencia* requerido para subsanar la opacidad de algunos sistemas, se exige una transparencia *suficiente* y no total¹⁴³, con el fin de evitar colisiones con los derechos de propiedad intelectual. Con esta declaración, la Comisión se posiciona claramente a favor del

¹⁴¹ FERNÁNDEZ ROZAS, J.C., *op.cit.*, p. 25.

¹⁴² Así se advierte en el Considerando 59 RIA.

¹⁴³ Para HUERGO LORA, A. «El proyecto de Reglamento sobre la Inteligencia Artificial», 2021. Disponible en <https://almacenedderecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial>, la regulación de la transparencia es una de las cuestiones más delicadas, y el proyecto busca un equilibrio en virtud del cual el proveedor debe mostrar cómo funciona la aplicación, incluida su «lógica general», así como los presupuestos de partida o una descripción de los datos que se hayan utilizado para su creación, pero no se le exige transparencia total sobre el *software* utilizado. Considera el autor, que «estos requisitos son, en cierto modo, “objetivos” máximos a los que se debe tender, pero que pueden conseguirse de muchas maneras y también con niveles de intensidad diferentes». En este sentido se pronuncia la *Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO* (2021), al considerar que el grado de transparencia y explicabilidad debería ser siempre adecuado al contexto y al efecto, ya que puede ser necesario encontrar un equilibrio entre la transparencia y la explicabilidad y otros principios como la privacidad, la seguridad y la protección (ap. 38).

equilibrio entre la necesidad de transparencia y los intereses empresariales, en la misma línea que ya venía manteniendo el Consejo de Europa. La versión inicial del RIA indicaba expresamente en su Exposición de Motivos que *ni siquiera las obligaciones que exigían una mayor transparencia debían afectar de manera desproporcionada a los derechos de propiedad intelectual* puesto que únicamente debían aplicarse a la información mínima necesaria para que las personas pudieran ejercer su derecho a una compensación efectiva y solo exigían la transparencia necesaria hacia las autoridades de supervisión y las encargadas de la aplicación de la ley. También se establecía que la información habría de divulgarse siempre con arreglo a la legislación pertinente en la materia, y que, tanto las autoridades públicas como los organismos notificados tendrían que cumplir obligaciones de confidencialidad vinculantes en los casos en que debieran tener acceso a información confidencial o al código fuente para examinar el cumplimiento de las obligaciones sustanciales¹⁴⁴. En la versión definitiva del RIA también se establece reiteradamente que toda la información o documentación a la que tengan acceso las autoridades, organismos notificados y cualquier otra persona física o jurídica que participe en su aplicación, deberá ser tratada de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

En segundo lugar, el *tipo y nivel de transparencia* exigible ha de ser compatible con el cumplimiento de las obligaciones legales de proveedores y responsables del despliegue.

En tercer lugar, el RIA *asocia la transparencia con la información que se debe suministrar al responsable del despliegue del sistema*. Es decir, en principio la obligación de transparencia y comunicación de información va dirigida a informar a los agentes que implementan la tecnología y no a las personas potencialmente afectadas por la decisión automatizada. Por tanto, se trata de una transparencia interna y no hacia los usuarios finales.

El Considerando 72 RIA da amplia cuenta de que el objetivo de la transparencia exigible a los sistemas de alto riesgo es que los responsables del despliegue puedan «*comprender la manera en que el sistema de IA funciona, evaluar su funcionalidad y comprender sus fortalezas y limitaciones*», así como «*utilizar el sistema y tomar decisiones con conocimiento de causa*». No obstante, como se explicará *infra*, esto repercutirá indirecta y favorablemente en la transparencia hacia los usuarios finales -transparencia externa- en la medida en que contribuirá a dar cumplimiento a las exigencias del art. 86 que obliga a los responsables a dar explicaciones a los afectados por la decisión del sistema.

¹⁴⁴ Apartado 3.5 de la Exposición Motivos que contenía la Propuesta de RIA de 21 de abril de 2021 -COM(2021) 206 final-.

Con estos fines, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas (en un formato digital o de otro tipo adecuado) e incluir información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda. Concretamente, en las instrucciones de uso el proveedor de la tecnología quedará obligado a informar al responsable del despliegue de forma adecuada y suficiente sobre una serie de extremos *mínimos* que se recogen en el art. 13.3, entre los que se incluyen, por ejemplo, las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo. Además, para facilitar que los responsables del despliegue comprendan dichas instrucciones, deberán contener ejemplos ilustrativos según proceda¹⁴⁵.

Por otro lado, otro requisito exigible por el RIA que también contribuye a la transparencia externa, es que los sistemas de alto riesgo deban *registrarse en una base datos de la UE* que la Comisión gestionará con el propósito de redoblar la transparencia y vigilancia públicas y de fortalecer la supervisión *ex post* por parte de las autoridades competentes (art. 49 en relación con el art. 71)¹⁴⁶. Como dispone el art. 71.4, la información de esta base de datos registrada de conformidad con lo dispuesto en el artículo 49 será accesible y estará a disposición del público de manera sencilla.

Por último, aunque no serán objeto de análisis en este trabajo, debe al menos mencionarse que los proveedores e implantadores de *modelos de IA de uso general*, quedan sometidos a obligaciones de transparencia más exigentes en virtud del RIA.

B) Determinados sistemas de IA con independencia de su riesgo

El art. 50 impone a proveedores y responsables del despliegue obligaciones de transparencia específicas respecto a ciertos sistemas de IA, con independencia de si son o no de alto riesgo¹⁴⁷. Se trata de aquellos destinados a interactuar directamente con personas físicas, sistemas que generen contenido sintético de audio, imagen, vídeo o texto, sistemas de reconocimiento de

¹⁴⁵ Considerando 72.

¹⁴⁶ Que el objetivo de esta obligación es aumentar la transparencia hacia el exterior o de cara al público lo expresa claramente el Considerando 131: «Con el objetivo de facilitar la labor de la Comisión y de los Estados miembros en el ámbito de la IA, así como de incrementar la transparencia de cara al público ...».

¹⁴⁷ En los Considerandos 132, 133 y 134 se justifica la imposición de tales obligaciones a estos sistemas.

emociones o de categorización biométrica y sistemas que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultrafalsificación, o generen o manipulen texto que se publique para informar sobre asuntos de interés público. En todos estos casos, se exceptúan de esta obligación los sistemas de IA autorizados legalmente para detectar, prevenir, investigar o enjuiciar delitos.

El objetivo que se persigue en estos casos con la transparencia e información es evitar la confusión o engaño de quienes interactúan o se ven expuestos a dichos sistemas¹⁴⁸. Para ello, en el primer caso, se deberá comunicar a las personas que están interactuando con un sistema de IA y no con un humano (excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización). Al aplicar dicha obligación, deben tenerse en cuenta las características de las personas físicas pertenecientes a colectivos vulnerables debido a su edad o discapacidad, en la medida en que el sistema de IA esté destinado a interactuar también con dichos colectivos.

En el segundo caso, se velará por que la información de salida del sistema esté marcada en un formato legible por máquina y que sea posible detectar que ha sido generada o manipulada de manera artificial y no por un ser humano. Se exige a los proveedores que integren soluciones técnicas y métodos para lograr este cometido que deberán ser lo suficientemente fiables, interoperables, eficaces y sólidos, en la medida en que sea técnicamente viable, teniendo en cuenta las técnicas disponibles o una combinación de dichas técnicas, como marcas de agua, identificación de metadatos, métodos criptográficos para demostrar la procedencia y la autenticidad del contenido, métodos de registro, impresiones dactilares u otras técnicas, según proceda. Además, a la hora de aplicar esta obligación, deberán tener en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes¹⁴⁹.

¹⁴⁸ Señala FERNÁNDEZ ROZAS, J.C., *op.cit.*, p. 16, que con los requisitos de transparencia que se imponen a los sistemas que interactúan con seres humanos se pretende dar lugar a un cambio significativo en las prácticas de divulgación a escala global en sitios web y aplicaciones, y garantizará que los usuarios estén informados sobre el funcionamiento y el propósito de los sistemas de IA con los que interactúan.

¹⁴⁹ Indica el Considerando 133 que «Dichas técnicas y métodos pueden implantarse a nivel de sistema de IA o a nivel de modelo de IA, incluidos modelos de IA de uso general que generan contenidos, facilitando así el cumplimiento de esta obligación por parte del proveedor posterior del sistema de IA. Para garantizar la proporcionalidad, conviene prever que esta obligación de marcado no se aplique a los sistemas de IA que desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica».

En el tercer caso, se notificará a las personas físicas que están expuestas a sistemas de IA que tratan sus datos biométricos y que pueden determinar o inferir sus emociones o intenciones, así como incluirlas en categorías específicas en función del sexo, edad, color del pelo o de ojos, tatuajes, rasgos personales, origen étnico o preferencias e intereses personales. Dichos datos personales se tratarán de conformidad con el Reglamento y la Directiva de protección de datos personales. Además, si las personas cuyos datos se tratan son personas con discapacidad, toda la información y notificaciones deberán facilitarse en formatos accesibles.

Por lo que se refiere al último tipo de sistemas mencionado, deberá hacerse público que los contenidos, imágenes o texto han sido generados o manipulados de manera artificial etiquetando los resultados de salida generados por la IA e indicando su origen artificial. No obstante, cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, sólo se deberá hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra, su explotación y uso normales, al tiempo que se conserva su utilidad y calidad¹⁵⁰.

Se exige inmediatez a la hora de revelar la información y que la misma se ajuste a los requisitos de accesibilidad aplicables. Así, toda información y notificaciones deberán facilitarse de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición al sistema (art. 50.5).

4.3.2. Derecho a una explicación

En la versión original del RIA, de 21 de abril de 2021, no se reconocía ningún derecho a ser informado de la existencia de decisiones automatizadas, ni un derecho de acceso a los datos o información del sistema, ni un derecho a recibir una explicación por su mal funcionamiento¹⁵¹. Es decir, no se recogían

¹⁵⁰ Se precisa con más detalle en el Considerando 134, que «el cumplimiento de esta obligación de transparencia no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida obstaculiza el derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, con sujeción a unas garantías adecuadas para los derechos y libertades de terceros [...] Además, también conviene prever una obligación de divulgación similar en relación con el texto generado o manipulado por una IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por la IA haya sido sometido a un proceso de revisión humana o de control editorial y que una persona física o jurídica ejerza la responsabilidad editorial de la publicación del contenido».

¹⁵¹ NAVAS NAVARRO, S., *Daños ocasionado...*, cit., p. 73.

en dicho instrumento derechos subjetivos para los afectados por dichas decisiones (usuarios finales), sino que sus previsiones iban dirigidas exclusivamente a los proveedores de tecnología basada en IA respecto a los responsables de su despliegue¹⁵². Esta carencia fue muy criticada por la doctrina y los organismos internacionales que la calificaron como un punto ciego de la regulación¹⁵³ y el Parlamento introdujo una enmienda en la que recogía un *derecho de explicabilidad algorítmica* muy similar al consagrado en el RGPD, pero con la importante diferencia de ser aplicable también a las *decisiones semiautomatizadas*, esto es, a aquellas que adopta una persona con apoyo en los resultados del sistema. De hecho, en el art. 68 *quarter*, titulado «Derecho a explicación de la toma individual de decisiones», se establecía que «toda persona afectada sujeta a una *decisión adoptada por el implementador* [ahora responsable del despliegue] *sobre la base de la información de salida de un sistema de IA de alto riesgo que produzca efectos jurídicos o que le afectan significativamente* de una manera que considera que perjudica a su salud, seguridad, derechos fundamentales, bienestar socioeconómico o cualquier otro de sus derechos derivados de las obligaciones establecidas en el presente Reglamento, *tendrá derecho a solicitar al implementador una explicación clara y significativa, de conformidad con el artículo 13, apartado 1, sobre el papel del sistema de IA en el procedimiento de toma de decisiones, los principales parámetros de la decisión adoptada y los datos de entrada correspondientes*». Añadiendo en el apartado tercero que dicho precepto se aplicaría *sin perjuicio de lo previsto en los artículos 13, 14, 15 y 22 del RGPD*¹⁵⁴.

El objetivo de dicha enmienda era subsanar la laguna de la que adolecía la normativa y conseguir que la transparencia algorítmica no sólo fuera

¹⁵² Nos remitimos a lo ya explicado *supra* sobre el art. 13.

¹⁵³ Entre los autores que critican dicha omisión del RIA: RIVAS VALLEJO, P., «Herramientas desde el derecho antidiscriminatorio...», *cit.*, p. 542, ÁLVAREZ CUESTA, H. «Inteligencia artificial: derecho de la UE y derecho comparado. La propuesta de una ley sobre IA», *cit.*, o MUÑOZ GARCÍA, C., «Adaptar o reformular la directiva 85/374 sobre responsabilidad por daños causados por productos defectuosos a la inteligencia artificial», accesible en <https://diariolaley.laleynext.es/dll/2022/03/01/adaptar-o-reformular-la-directiva-85-374-sobre-responsabilidad-por-danos-causados-por-productos-defectuosos-a-la-inteligencia-artificial>. Según la Recomendación de la UNESCO (ap. 38), las personas deben estar plenamente informadas cuando una decisión se basa en algoritmos de IA o se toma a partir de ellos, en particular cuando afecta a su seguridad o derechos humanos y deben tener la oportunidad de solicitar explicaciones e información al actor de la IA o a las instituciones públicas correspondientes. Además, deben poder conocer los motivos por los que se ha tomado una decisión que afecta a sus derechos y libertades y tener la posibilidad de presentar alegaciones a fin de que se revise y enmiende la decisión.

¹⁵⁴ El apartado segundo del art.68 *quarter* establecía excepciones a la aplicación de este derecho de explicación a disponer que «El apartado 1 no se aplicará a la utilización de sistemas de IA para los que el Derecho nacional o de la Unión prevea excepciones o restricciones a la obligación prevista en el apartado 1 en la medida en que dichas excepciones o restricciones respeten la esencia de los derechos y libertades fundamentales y sean una medida necesaria y proporcionada en una sociedad democrática»

dirigida a los operadores de la tecnología sino también a las personas físicas afectadas por las decisiones automatizadas. Tras dicha enmienda, la versión del texto aprobada el 13 de marzo de 2024 por la Eurocámara¹⁵⁵ recogió por primera vez ese *derecho de las personas afectadas a obtener una explicación de las decisiones individuales*, novedad importante respecto de la que no se produjeron modificaciones tras su aprobación definitiva en mayo de ese mismo año.

Dispone ahora literalmente el art. 86 que «Toda persona que se vea afectada por una *decisión que el responsable del despliegue adopte basándose en los resultados de un sistema de IA de alto riesgo* que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y *que produzca efectos jurídicos o le afecte considerablemente del mismo modo*, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, *tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada*». Se consagra expresamente un derecho de explicación *ex post*, central en la ordenación de la IA, que viene a completar el limitado y criticable ámbito del art. 22 RGPD por cuanto se aplica a los sistemas de apoyo a la decisión y no sólo a los que tomen decisiones de forma totalmente automatizada.

Se establecen dos límites a la aplicación de este derecho: el primero, que no se aplicará cuando se utilicen sistemas de IA para los que existan excepciones o restricciones a la obligación prevista en el apartado 1 derivadas del Derecho nacional o de la UE (art. 86.2); el segundo, que solo se aplicará en la medida en que no esté ya previsto en el Derecho de la Unión (art. 86.3), disposición que contiene una clara referencia al RGPD.

Dicho derecho se completa con la obligación de los responsables del despliegue establecida en el nuevo art. 26.11, en virtud de la cual, en el caso de que se estén utilizando sistemas de IA de alto riesgo del anexo III que *tomen decisiones o ayuden a tomar decisiones* relacionadas con personas físicas, *deberán informar a dichas personas de que están expuestas a la utilización de tales sistemas*, sin perjuicio de lo dispuesto en el art. 50 sobre obligaciones de transparencia específicas cuando se usen determinados sistemas IA destinados a interactuar con personas físicas¹⁵⁶. Por tanto, es evidente que los responsables del despliegue asumen un papel fundamental a la hora de garantizar la transparen-

¹⁵⁵ P9TA(2024)0138. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

¹⁵⁶ También dispone el art. 26.11 que «En el caso de los sistemas de IA de alto riesgo que se utilicen a los efectos de la aplicación de la ley, se aplicará el artículo 13 de la Directiva (UE) 2016/680».

cia externa hacia las personas afectadas por los sistemas tanto antes (*ex ante*) como después de adoptada la decisión (*ex post*). Respecto a la primera, porque deben informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo, información que debe incluir tanto la finalidad prevista como el tipo de decisiones que se toman. Respecto a la segunda, porque deben informarles de que gozan de un derecho a obtener una explicación de la decisión y darle cumplimiento.

De todo esto se infiere que, igual que dijimos respecto del RGPD, el RIA también pretende superar los dos niveles de opacidad algorítmica a los que se hizo referencia en el apartado 2. Por un lado, garantizando la transparencia *sobre el uso* de dichos sistemas para que los ciudadanos sean conscientes de que es una IA la que decide sobre su persona; por otro lado, garantizando la transparencia *sobre el contenido* y justificación de la decisión final.

Por lo que se refiere al contenido concreto de la explicación que debe ofrecer el responsable al afectado por la decisión, dos son los extremos sobre los que ha de informarle: en primer lugar, del papel que el sistema de IA ha tenido en el proceso de toma de decisiones; y en segundo lugar, de los principales elementos de la decisión adoptada. Deberá hacerlo de forma clara y significativa, es decir, de forma suficiente para que el afectado pueda ejercer sus derechos.

Dar explicaciones sobre el *papel que ha jugado el sistema* a la hora de tomar la decisión implicará informar al interesado sobre si se trata de una decisión plena o semiautomatizada, es decir, si el resultado se ejecutó de forma totalmente automática y sin intervención humana, o si se utilizó como mero apoyo de la decisión adoptada finalmente por una persona. Además, en este último caso tendrá que indicar también si el resultado del sistema fue *determinante o no* para la toma de la decisión final y en qué medida lo fue¹⁵⁷.

De hecho, la cuestión de hasta qué punto la salida o resultado del sistema de IA es *determinante* para la decisión finalmente adoptada por el usuario, ya no es solo relevante a los efectos de aplicar las garantías del art. 22 RGPD, sino que ahora también es decisiva para determinar si un sistema de IA es considerado de alto riesgo y, en consecuencia, para la aplicación de todas las garantías previstas en el RIA¹⁵⁸. Es decir, los sistemas de IA independientes se clasifican

¹⁵⁷ Sobre el carácter «determinante» o no del resultado del sistema para la toma de la decisión final nos remitimos a las apreciaciones realizadas al comentar *supra* la STJUE de 7 de diciembre de 2023.

¹⁵⁸ Así lo aprecia con acierto COTINO HUESO, «La primera sentencia del Tribunal de Justicia de la Unión Europea...», cit., para quien, la relevancia del resultado del sistema de IA en la decisión finalmente adoptada ha pasado a ser en el RIA un elemento esencial para determinar si el sistema es de alto riesgo.

como de alto riesgo si, a la luz de su *finalidad prevista*, presentan un *alto riesgo de ser perjudiciales para la salud y la seguridad o los derechos fundamentales de las personas*, teniendo en cuenta tanto la *gravedad* del posible perjuicio como la *probabilidad* de que se produzca, y se utilizan en una serie de ámbitos especificados en el Reglamento. No obstante, tal como se explica en el Considerando 53, pueden existir casos en los que, a pesar de utilizarse en esos ámbitos predefinidos, los sistemas no entrañen un riesgo considerable de causar perjuicios a intereses jurídicos protegidos *si no influyen sustancialmente en la toma de decisiones*. Se entenderá que no influyen sustancialmente en la toma de decisiones cuando no afecten al fondo, ni por consiguiente al resultado, de la toma de decisiones humana o automatizada. Las condiciones (una o varias) para que pueda considerarse que un sistema no plantea dicho riesgo al no influir sustancialmente en el resultado de la toma de decisiones, se recogen en el art. 6.3. Su concurrencia implicará que esos sistemas no queden sometidos a los requisitos que el RIA impone a los sistemas de alto riesgo.

Respecto a los *principales elementos de la decisión adoptada*, creemos que podría aplicarse aquí lo explicado en el apartado 4.2.2 sobre el contenido del derecho de información reforzado en el RGPD. Así, habría que informar, entre otras cosas, de los factores utilizados por el algoritmo para tomar la decisión o la elaboración del perfil, la ponderación relativa de cada variable en el modelo para la toma de la decisión y cualquier cambio de estos parámetros que modifique el comportamiento del algoritmo, las reglas e instrucciones utilizadas por el algoritmo, así como los datos utilizados por el sistema respetando en todo caso el RGPD.

A nuestro modo de ver, debe aplaudirse que el RIA haya acabado consagrando este derecho a favor de los potenciales afectados por las decisiones de la IA en la medida en que contribuirá a que comprendan cómo se adoptan y cómo pueden afectarles. A este fin contribuye también la exigencia del RIA de educar y formar en competencias de IA a todos los que operan con ella. En su art. 4, titulado «Alfabetización en materia de inteligencia artificial» se establece que «*Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal¹⁵⁹ y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta*

¹⁵⁹ Asimismo, los responsables del despliegue deben garantizar que las personas encargadas de poner en práctica las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan las competencias necesarias, en particular un nivel adecuado de alfabetización, formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas. Dichas obligaciones deben entenderse sin perjuicio de otras obligaciones que tenga el responsable del despliegue en relación con los sistemas de IA de alto riesgo con arreglo al Derecho nacional o de la Unión (Considerando 91).

sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los grupos de personas en que se utilizarán dichos sistemas»¹⁶⁰.

En el Considerando 20 se explica con más detalle que, con el fin de aprovechar las ventajas de estos sistemas y proteger al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, la alfabetización en IA debe dotar a proveedores, responsables del despliegue y personas afectadas, de los conceptos necesarios para *tomar decisiones con conocimiento de causa en relación con los sistemas de IA*¹⁶¹. Por lo que se refiere concretamente a estas últimas, se les debe dotar de los *conocimientos necesarios para comprender el modo en que las decisiones adoptadas con la ayuda de la IA tendrán repercusiones para ellas*.

Dicha formación será importante, además, para que cualquier persona que deba tomar decisiones basadas en resultados algorítmicos pueda hacer frente de forma eficaz al peligroso sesgo de la automatización¹⁶². Asimismo, estos conocimientos previos permitirán, posteriormente, implementar otras medidas desde el ámbito de la tecnología para abordar el sesgo de estos sistemas, y en particular, el sesgo en los datos que los alimentan, el cual se erige como principal causa de la discriminación algorítmica. En definitiva, con esta alfabetización en IA se pretende, por un lado, proporcionar a todos los agen-

¹⁶⁰ El art.3, ap. 56, define la «alfabetización en materia de inteligencia artificial» como «las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la inteligencia artificial, así como de los perjuicios que puede causar». Además, se establece que el Comité Europeo de Inteligencia Artificial deberá apoyar a la Comisión para promover las herramientas de alfabetización en IA, la sensibilización pública y la comprensión de los beneficios, riesgos, salvaguardias, derechos y obligaciones en relación con el uso de sistemas de IA (vid., art. 66 «Funciones del Comité», concretamente, el ap. f), y que tanto la Comisión como los Estados miembros deberán facilitar la elaboración de códigos de conducta voluntarios para promover dicha alfabetización entre las personas que se ocupan del desarrollo, manejo y uso de la IA (vid., art. 95.c).

¹⁶¹ Estos conceptos pueden variar en función del contexto pertinente e incluir el entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar la información de salida del sistema de IA y, en el caso de las personas afectadas, los conocimientos *necesarios para comprender el modo en que las decisiones adoptadas con la ayuda de la IA tendrán repercusiones para ellas*.

¹⁶² Para SORIANO ARNANZ, A./SIMÓ SOLER, E. (2021), «Machine learning y Derecho: aprendiendo la (des)igualdad», en *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, S. Barona Vilar (ed.), Valencia, p. 203, la ventaja de que jueces y magistrados estén debidamente formados en perspectiva de género no se limita a que sus pronunciamientos carezcan de prejuicios negativos, sino que cumple una función preventiva y de detección de argumentos estereotipados por parte de los empresarios que utilizan sistemas de IA para la toma de decisiones, como de los propios programadores que introducen las instrucciones, variables y datos.

tes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento y la correcta ejecución del RIA, y por otro lado, que tanto la sociedad en general como sobre todo los que se encargan de diseñar, desarrollar, desplegar o usar estos sistemas, tomen conciencia de sus características, forma de funcionamiento, ventajas y potenciales riesgos. Todo ello coadyuvará a consolidar el camino hacia una IA fiable.

5. CONSIDERACIONES FINALES SOBRE LA NECESIDAD DE TRANSPARENCIA Y EXPLICABILIDAD PARA DETECTAR Y DEMOSTRAR LA DISCRIMINACIÓN ALGORÍTMICA

La transparencia ha sido una cuestión prioritaria a la que se ha dedicado especial atención por las instituciones y la doctrina desde los inicios del tratamiento regulatorio de la IA. De hecho, se ha erigido en un principio básico de muchos marcos normativos, éticos y de seguridad vigentes y proyectados. Es lógico, por ello, que también sea uno de los pilares básicos sobre los que se asienta el reciente Reglamento europeo que regula la materia y con el que se pretende fomentar la confianza en los sistemas inteligentes y mitigar riesgos como el sesgo y la discriminación injusta al que se ha hecho especial referencia en este trabajo.

Si bien es cierto que la transparencia no puede impedir que los sistemas de IA lleguen a resultados errados y/o discriminatorios, ni garantizar su equidad y justicia, es fundamental para descubrir desviaciones que pasarían desapercibidas si no se exigiera tanto en el diseño como en el despliegue y uso de los sistemas de IA. Dicha exigencia debe operar en todo el ciclo de vida de los sistemas y ha de ser tanto interna como externa.

Es más, no solo ha de abogarse porque los sistemas sean transparentes, sino también, y sobre todo, porque sus resultados sean explicables. Mientras la transparencia tiene que ver con el proceso seguido para llegar a un resultado, y pretende dar a conocer y entender cómo se procesa el dato que se introduce en el sistema, la explicabilidad tiene que ver con el resultado de ese proceso y descende más al detalle¹⁶³. Por tanto, de lo que se trataría con la explicabilidad sería de que el afectado por la decisión pudiera conocer los motivos por los que se ha tomado una decisión que afecta a sus derechos y libertades y tuviera la posibilidad de impugnarlas. No sería suficiente con dar una explicación genérica sobre cómo funciona el proceso de toma de decisión, sino que

¹⁶³ Así lo afirma el Director del Centro Europeo para la Transparencia Algorítmica (ECAT), Alberto Pena Fernández, en Diario La Ley, 8 de marzo de 2024.

habría que indicar los datos específicos de la persona en base a los cuales se ha tomado una decisión o se ha hecho un perfilado. En definitiva, no solo habría que informar de forma clara y sencilla de la denominada «lógica computacional» del sistema, sino también de su «lógica decisional». Sólo así podrán salvaguardarse derechos fundamentales como la tutela judicial efectiva, el derecho a la defensa o la igualdad y no discriminación.

En este sentido, es elogiable que el RIA haya acabado acogiendo un *derecho a la explicación* que viene a completar tanto las previsiones sobre transparencia y comunicación de información entre los diversos sujetos de la cadena de valor (principalmente, entre proveedores y responsables del despliegue) que ya preveía su versión inicial, como el insuficiente y criticado alcance del art. 22 RGPD que suponía una importante traba en la lucha contra la opacidad de los sistemas de IA.

Asimismo, cuando las decisiones se basan en datos personales, el control sobre nuestra información personal ha de implicar la posibilidad de ejercer, como mínimo, una serie de derechos como el de ser informados sobre el razonamiento subyacente al procesamiento de datos realizado por los algoritmos, el derecho a oponerse a dicho procesamiento y el derecho a recurrirlo. Ello no sólo cuando se trate de decisiones plenamente automatizadas sino también semiautomatizadas.

En definitiva, tanto la transparencia como la explicabilidad de los sistemas de IA que toman decisiones basadas en datos personales y con efectos jurídicos en personas concretas son cruciales para que la ciudadanía confíe en ellos. Deben articularse medidas para hacer frente a la opacidad algorítmica tanto desde el ámbito jurídico, como desde el terreno ético y por supuesto tecnológico, tratando de encontrar un equilibrio adecuado entre las exigencias requeridas para proteger la salud, seguridad y derechos fundamentales de las personas y los intereses empresariales. Sin duda, tanto la aprobación definitiva del RIA, como la nueva interpretación del TJUE sobre el ámbito de aplicación del art. 22 RGPD, suponen pasos en firme para conseguirlo.

BIBLIOGRAFÍA

- ALAMEDA CASTILLO, M.T., «Reclutamiento tecnológico. Sobre algoritmos y acceso al empleo», *Temas laborales: Revista andaluza de trabajo y bienestar social*, N° 159, 2021, pp. 11-52.
- ALCOLEA AZCÁRRAGA, C., «La responsabilidad patrimonial de la Administración y el uso de algoritmos», *Revista General de Derecho Administrativo*, n° 59, enero 2022. Recuperado de <https://laadministracionaldia.inap.es/noticia.asp?id=1512629>

- ÁLVAREZ CUESTA, H. «Inteligencia artificial: derecho de la UE y derecho comparado. La propuesta de una ley sobre IA», en P. Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, pp. 379-414.
- ARCOS VARGAS, M., «La no discriminación en el Derecho derivado de la Unión Europea» en J.M. MORALES ORTEGA (dir.), *Realidad social y discriminación. Estudios sobre diversidad e inclusión laboral*, Murcia, 2022, pp. 17-41.
- ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, 2022.
- BARRIOS ANDRÉS, M., *Manual de Derecho Digital*, Valencia, 2020.
- BAZ LOMBA, C. (2021). Los algoritmos y la toma de decisiones administrativas. Especial referencia a la transparencia. *Revista CEFLegal*, 243, 119-160.
- BELTRÁN DE HEREDIA, I., «Automatización y obsolescencia humana», en *Retos jurídicos de la inteligencia artificial*, coord. por Agustí Cerrillo i Martínez y Miquel Peguera Poch, 2020, pp. 113-124.
- BIBAL A./LOGNOUL, M./DE STREEL, A./FRÉNAY, B., «Legal requirements on explainability in machine learning», *Artificial Intelligence & Law*, 29(2), 2021, pp. 149-169.
- CASADESÚS RIPOLL, P., *La responsabilidad civil por el uso discriminatorio de los datos personales a través de la inteligencia artificial*, Granada, 2022.
- CASTELLANOS CLARAMUNT, J., «Derecho e inteligencia artificial: atención especial a los sesgos, la privacidad y la protección de datos», accesible en <https://idpbarcelona.net/derecho-e-inteligencia-artificial-atencion-especial-a-los-sesgos-la-privacidad-y-la-proteccion-de-datos/>
- CASTILLA, K., *Cuatro ángulos de análisis de la igualdad y la no discriminación en la inteligencia artificial*, Barcelona, 2022, <https://www.idhc.org/arxius/recerca/Inteligencia-artificial-vF.pdf>
- CASTILLO OCARANZA, C., «Discriminación algorítmica en el ámbito laboral», en P. Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, pp. 71-78.
- CASTILLO PARRILLA, J.A., «Sentencia del Tribunal Ordinario de Bolonia de 31 de diciembre de 2020 (Caso Deliveroo) ¿Discriminación algorítmica o discriminación a través de un algoritmo?», *Derecho Digital e Innovación. Digital Law and Innovation Review*, n.7 (octubre-diciembre), 2020.
- CONSEJO DE EUROPA, *Manual de legislación europea contra la discriminación (edición 2018)*, Luxemburgo, 2019.
- COTINO HUESO, L., «La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial» *Diario LA LEY*, N° 80, Sección Ciberderecho, 17 de Enero de 2024.
- «Caso Bosco, a la tercera tampoco va la vencida. Mal camino en el acceso los algoritmos públicos», *Diario LA LEY*, N° 84, Sección Ciberderecho, 17 de Mayo de 2024.

- «Transparencia de la inteligencia artificial pública: marco legal, desafíos y propuestas», *Actualidad Administrativa*, N° I, Sección Actualidad, Diciembre 2023.
- DE LA NUEZ SÁNCHEZ CASCADO, E., «Algoritmos y transparencia», disponible en <https://www.hayderecho.com/2020/02/18/algoritmos-y-transparencia-2/>.
- EGUÍLUZ CASTAÑEIRA, J.A., «Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales», *Estudios de Deusto: revista de Derecho Público*, vol. 68, n. 2, 2020, pp. 325-367.
- EUBANKS, V., *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, St MARTÍN's Press, 2018.
- EVANGELIO LLORCA, R., «Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por N. Álvarez Lata; J.M. Busto Lago (pr.), 2024, pp. 549-619.
- FERNÁNDEZ DE LA MORENA, B., *Discriminación algorítmica. Estudio del sesgo en arquitecturas de aprendizaje profundo*, Madrid, 2019.
- FERNÁNDEZ ROZAS, J.C., «La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo», LA LEY Unión Europea, N° 124, Sección Estudios, Abril 2024, LA LEY 15196/2024.
- GASCÓN MARCÉN, A., «Derechos humanos e inteligencia artificial», en *Setenta años de Constitución Italiana y cuarenta años de Constitución Española*, Pérez Miras (dir.), Teruel Lozano (dir.), Raffiotta (dir.), Pia Iadicco (dir.), Vol. 5, 2020 (Retos en el siglo XXI / coord. por Silvia Romboli), pp. 335-350.
- GERARDS, J./ XENIDIS, R., *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law* (Special report European network of legal experts in gender equality and non-discrimination), European Commission, 2020.
- GIL MEMBRADO, C., «Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra», en N. Álvarez Lata/J.M. Busto Lago, *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, 2024, pp. 501-547.
- GINÈS i FABRELLAS, A., «Sesgos discriminatorios en la automatización de decisiones en el ámbito laboral: evidencias de la práctica», en RIVAS VALLEJO, P. (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra, 2022, pp. 295-332.
- GONZÁLEZ VALVERDE, A., «Responsabilidad por el potencial de sesgo discriminatorio de los algoritmos de los productos de Inteligencia Artificial. A propósito de la Algorithmic Accountability Act of 2019 (s.1108)». En Ataz López y Cobacho Gómez, *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón*, Vol. 2, 2021, pp. 1225-1273.
- GOODMAN, B./FLAXMAN, S., «European Union regulations on algorithmic decision-making and a “right to explanation”», presented at ICML Workshop on Human Interpretability in Machine Learning, New York, 2016, <https://arxiv.org/abs/1606.08813v3>.

- HERRERA DE LAS HERAS, R., «Protección de datos e inteligencia artificial», en Cruz Blanca/Lledó Benito (coords.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, 2021, pp. 644-669.
- HUERGO LORA, A., «Una aproximación a los algoritmos desde el derecho administrativo», en A. HUERGO LORA (dir.) y G. DÍAZ GONZÁLEZ (coord.), *La regulación de los algoritmos*, Navarra, 2020, pp. 23-87.
- «El proyecto de Reglamento sobre la Inteligencia Artificial», *Almacén del Derecho*, 17 de abril de 2021.
- «Por qué aciertan las sentencias sobre el ‘algoritmo’ del bono social eléctrico», *Almacén del Derecho*, 10 de mayo de 2024.
- LAZCOZ MORATINOS, G., «Análisis jurídico de la toma de decisiones algorítmica en la asistencia sanitaria», en *La regulación de los algoritmos*, coord. por Gustavo Manuel Díaz González; Alejandro José Huergo Lora (dir.), 2020, pp. 283-297.
- LÓPEZ-TARRUELLA MARTÍNEZ, A., *Propiedad intelectual e innovación basada en los datos*, Navarra, 2021.
- LLORENS ESPADA, J., «Responsabilidades civiles por discriminación por razón de género cuando medie un sistema de inteligencia artificial», en Rivas Vallejo (dir.), *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, pp. 573-602.
- MANHEIM, K. M., & KAPLAN, L., «Artificial Intelligence: Risks to Privacy and Democracy», *Yale Journal of Law and Technology* 106, vol. 21, 2019, pp. 106-189.
- MEDINA GUERRERO, M., «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales», *Teoría y realidad constitucional*, n° 49, 2022, pp. 141-171.
- MERCADER UGUINA, J.R. «Discriminación algorítmica y derecho granular: nuevos retos para la igualdad en la era del big data», *Labos: Revista de Derecho del Trabajo y Protección Social*, vol. 2, n. 2, 2021, pp. 4-10.
- MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, *Información algorítmica en el ámbito laboral. Guía Práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral*, mayo 2022.
- MUÑOZ GUTIÉRREZ, C., «La discriminación en una sociedad automatizada: Contribuciones desde América Latina», *Revista chilena de derecho y tecnología*, 10(1), 2021, pp. 271-307.
- MUÑOZ GARCÍA, C., «Adaptar o reformular la directiva 85/374 sobre responsabilidad por daños causados por productos defectuosos a la inteligencia artificial», *Revista Crítica de Derecho Inmobiliario*, Año 98, n° 793, 2022, pp. 2886-2908.
- NAVAS NAVARRO, S., *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Granada, 2022.
- «La perspectiva de género en la inteligencia artificial», *Diario La Ley*, n° 48, Sección Ciberderecho, 8 de marzo de 2021.

- «Sistemas expertos basados en inteligencia artificial y responsabilidad civil. Algunas cuestiones controvertidas», *Diario La Ley*, 13 de Diciembre de 2019, LA LEY 14980/2019.
- NÚÑEZ SEOANE, J., «El derecho a la información y acceso al funcionamiento de los algoritmos que tratan datos personales», en *La regulación de los algoritmos*, coord. por Gustavo Manuel Díaz González y Alejandro José Huergo Lora (dir.) 2020, pp. 299-315.
- O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Madrid, 2017.
- OTTOLIA, A., *Derecho, Biga Bata e Inteligencia Artificial*, Valencia, 2018.
- PALMA ORTIGOSA, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos», *Revista General de Derecho Administrativo*, n. 50, 2019.
- REBOLLO DELGADO, L. *Inteligencia artificial y derechos fundamentales*, Madrid, 2023.
- RIVAS VALLEJO, P., «Sesgos de automatización y discriminación algorítmica», en *Discriminación algorítmica en el ámbito laboral*, Pilar Rivas Vallejo (dir.), 2022, pp. 31-68.
- «Análisis desde el derecho antidiscriminatorio», en P. Rivas Vallejo (dir.) *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, pp.415-476.
- «Herramientas desde el derecho antidiscriminatorio y la protección frente a la igualdad y a la no discriminación», en P. Rivas Vallejo (dir.) *Discriminación algorítmica en el ámbito laboral*, Navarra 2022, pp. 539-572.
- RUBÍ PUIG, A., «Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores», *Revista De Educación Y Derecho*, 24, 2021.
- SÁEZ LARA, C., «El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación», *Temas laborales: Revista andaluza de trabajo y bienestar social*, N° 155, 2020, pp. 41-60.
- SÁNCHEZ CAPARRÓS, M. «Prevenir y controlar la discriminación algorítmica», 2022. https://www.researchgate.net/publication/358207305_Prevenir_y_controlar_la_discriminacion_algoritmica
- SELBST, A. D./POWLES, J., «Meaningful information and the right to explanation», *International Data Privacy Law*, 2017, Vol. 7, n.º 4, pp. 233 y ss.
- SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal: los sistemas algorítmicos de evaluación de riesgos», en *Dimensiones éticas y jurídicas de la inteligencia artificial en el marco del Estado de Derecho*, J.I. Solar Cayón (ed.), Alcalá de Henares, 2020, pp. 125-172.
- SORIANO ARNANZ, A. «Decisiones automatizadas y discriminación: aproximación y propuestas generales», *Revista General de Derecho Administrativo*, n. 56, 2021.
- «La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial», en *Nuevas normativas: inteligencia artificial, derecho y género* (coord. por P.R. Bonorino Ramírez / R. Fernández Acevedo / P. Valcárcel Fernández), Navarra, 2022, pp. 63-88.

- SORIANO ARNANZ, A./SIMÓ SOLER, E., «Machine learning y Derecho: aprendiendo la (des)igualdad», en S. Barona Vilar (ed.) *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Valencia, 2021, pp. 183-207.
- SUBERBIOLA GARBIZU, I., «Inteligencia artificial, opacidad y motivación de las decisiones administrativas automatizadas», en *La protección de los derechos fundamentales en el ámbito tributario*, coord. por Antonio Vázquez del Rey Villanueva e Irune Suberbiola Garbizu y dir., por Isaac Merino Jara, 2021, pp. 291-328.
- TOLOSA, P./DIBO, C., «Inteligencia artificial, discriminación por género y Derecho: viejos problemas, nuevos desafíos», en C. Danesi (dir.) *Inteligencia Artificial, tecnologías emergentes y Derecho*, 2021, pp. 155-190.
- VESTRI, G., «La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativ», *Revista Aragonesa de Administración Pública*, n° 56, 2021, pp. 368-398.
- WACHTER, S., MITTELSTADT, B., y FLORIDI, L. «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», *International Data Privacy Law*, Vol. 7, n. 2, 2017, pp. 1-47.

Aplicaciones de la inteligencia artificial conforme a la Ley de Movilidad Sostenible.

Consideraciones en torno al régimen de responsabilidad civil acorde con la innovación

YOLANDA BUSTOS MORENO

*Profesora Titular de Derecho Civil
Universidad de Alicante*

Sumario¹: 1. El Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial (AIA) y el Proyecto de Ley de Movilidad Sostenible de 23 de febrero de 2024. 1. Consideraciones generales de la AIA. 1.2. La regulación y su papel de apoyo a la innovación en el desarrollo de sistemas de IA. 1.3. El Proyecto de Ley de Movilidad Sostenible de 23 de febrero de 2024 con relación a la aplicación de la IA en vehículos automatizados (PLMS). 1.4. El concepto de “sistema de inteligencia artificial” en la AIA y PLMS. 2. Dilemas en torno a la regulación de la responsabilidad civil en las actividades que emplean sistemas de IA. 2.1. Características especiales de los sistemas de IA con relación al riesgo. 2.2. El debate sobre el régimen de responsabilidad civil más favorable a la innovación en sistemas de IA. 2.3. El replanteamiento de la responsabilidad objetiva en el *Complementary Impact Assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence*. 3. El apoyo a los sistemas de IA innovadores antes de la introducción en el mercado o puesta en servicio desde el perfil de la responsabilidad civil. Bibliografía.

¹ El trabajo se enmarca en el Proyecto Excelencia Prometeo “La nueva era de los algoritmos y la inteligencia artificial y su tutela jurídico-privada en el marco de la Unión Europea”, Referencia: CIPROM/2022/40 y en el Proyecto “La irrupción de la Inteligencia Artificial en el Derecho de daños y su adaptación a las nuevas tecnologías”, Referencia: PID2020-116185GB-I00.

1. EL REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 13 DE JUNIO DE 2024 POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL Y EL PROYECTO DE LEY DE MOVILIDAD SOSTENIBLE DE 23 DE FEBRERO DE 2024

1.1. CONSIDERACIONES GENERALES DE LA AIA

En 2019, cuando la inteligencia artificial (IA) comenzaba a ganar relevancia entre el público general, uno de los principales expertos en la materia, el profesor de Berkeley Stuart Russell, destacaba en su libro *Human Compatible* que «inevitablemente, la industria tecnológica deberá reconocer que sus productos tienen un impacto; y si lo tienen, es fundamental que esos productos no causen efectos nocivos. Esto implica que habrá normativas que regulen las interacciones de la IA con los humanos», llegando incluso a prohibir diseños que puedan generar efectos perjudiciales². Dentro de este contexto, el 12 de julio de 2024 el Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), también denominada “Ley de Inteligencia Artificial”, a la que en adelante nos referiremos como AIA (atendiendo a sus siglas en inglés), fue publicada en el DOUE, con entrada en vigor el 1 de agosto³. En efecto, tras el acuerdo político alcanzado en diciembre de 2023 entre el Parlamento, la Comisión y el Consejo, esta AIA se presenta como la primera normativa mundial en abordar los riesgos de la IA desde una perspectiva transversal, basada en riesgos abstractos y no vinculados a sectores específicos. Sin embargo, la UE es plenamente consciente de que la IA no debe ser tratada únicamente desde la óptica de los límites regulatorios. Por ello, la AIA incluye una serie de medidas destinadas a impulsar la innovación. A este respecto, destacan los espacios controlados de pruebas o *sandboxes* regulatorios, que permiten experimentar con nuevos productos sin temor a sanciones regulatorias, incluyendo facilidades de cumplimiento para pequeñas y

² Como describe García Mexía, P. “Europa ante el reto de la inteligencia artificial”, *The Objective*, 3-8-2024, <https://theobjective.com/tecnologia/2024-08-03/europa-ante-el-reto-de-la-inteligencia-artificial/>.

³ Aunque con distintas fases de aplicación (art. 113 AIA), como no podía ser de otro modo dada la envergadura de la puesta en práctica de sus disposiciones.

medianas empresas. Asimismo, se introducen pautas -aunque limitadas- para fomentar la investigación y la estandarización⁴.

La Comisión Europea en la Comunicación «Impulso a las empresas emergentes y la innovación en inteligencia artificial fiable»⁵ establece que, para evaluar adecuadamente el desempeño de los algoritmos en diferentes escenarios, conjuntos de datos y situaciones extremas, es esencial que los procedimientos de prueba sean rigurosos. Estos procedimientos permiten identificar y corregir sesgos en los datos de entrenamiento, así como prevenir, entre otros problemas, la generación de contenido inapropiado. Con este fin, la Comisión ha implementado diversas iniciativas para facilitar la prueba de algoritmos de IA en entornos reales, mediante la creación de instalaciones de ensayo y experimentación. Estas instalaciones, tanto virtuales como físicas, están diseñadas para ser utilizadas en sectores como la agroindustria, la manufactura, la salud y las ciudades inteligentes.

Asimismo, en el marco de la AIA, se prevé que los Estados miembros establezcan espacios controlados de pruebas para la IA proporcionando un entorno regulado donde las startups y empresas emergentes puedan desarrollar, probar y validar sistemas de IA innovadores bajo la supervisión de las autoridades competentes. Por otro lado, el Programa Europa Digital, a partir de 2024, brindará apoyo para el desarrollo de herramientas que permitan probar y validar modelos de IA, las cuales serán implementadas en las instalaciones de ensayo y los espacios de pruebas controladas. Finalmente, durante el período 2024-2027, la Comisión Europea, a través del programa Horizonte Europa, financiará proyectos que impulsen las capacidades de la IA generativa. Estos proyectos están enfocados para permitir que la IA combine de manera eficaz aportaciones multimodales y fomente nuevos enfoques de aprendizaje innovadores, contribuyendo así al avance de las futuras generaciones de sistemas de IA⁶.

⁴ Paralelamente a estos pasos regulatorios, la UE ha puesto en marcha iniciativas que buscan mejorar la competitividad en el campo de la IA. En este contexto, se enmarca el “Paquete de Innovación en IA”, acordado en enero de 2024, que tiene como objetivo principal promover la inversión y fortalecer nuestras capacidades de computación, elementos imprescindibles para el desarrollo de la IA. En el mismo se recuerda que tres superordenadores europeos están entre los diez mayores del mundo (Leonardo, Lumi y Mare Nostrum 5, este último en Barcelona), *ibid.* Nota 2. Véase también el documento de la European Commission: “Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme”, disponible en: <https://digital-strategy.ec.europa.eu/en/activities/testing-and-experimentation-facilities>

⁵ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on boosting startups and innovation in trustworthy artificial intelligence, COM/2024/28 final, pp. 9-10, <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52024DC0028>

⁶ Para más información al respecto, pueden consultarse los artículos de mi autoría: BUSTOS MORENO, Y. “La responsabilidad civil en los espacios controlados de pruebas (regulatory sand-

1.2. LA REGULACIÓN Y SU PAPEL DE APOYO A LA INNOVACIÓN EN EL DESARROLLO DE SISTEMAS DE IA

Partiendo del verdadero esfuerzo comunitario por impulsar la competitividad que hemos expuesto, debe reconocerse que la realidad económica no es muy prometedora en Europa. En efecto, según datos de 2024 de la OCDE⁷, más del 90% de la inversión mundial de capital-riesgo en IA, que se disparó de 2.700 millones de euros en 2022 a 24.000 millones de euros en 2023, se ve materializada en Estados Unidos. La UE solo cuenta con nueve empresas entre las 100 mayores digitales del mundo (España tiene una), frente a 58 que son estadounidenses. Y además con la particularidad de que, entre los 16 mayores modelos de IA generativa del mundo, solo hay uno europeo (francés en concreto), siendo los otros 15 de los EE UU. Pues bien, al amparo de este contexto económico, se habla del efecto “Bruselas” al efecto “Delaware”⁸ y en esta línea, no sorprende que recientemente el Informe *Dragui* “The future of European competitiveness”⁹, declare que alrededor del 70% de la brecha en el PIB per cápita con Estados Unidos en términos de PPA, se explica por la menor productividad en la UE¹⁰. Y respecto al contexto europeo, se desprende de la idea de que existe una falta de conexión entre la innovación y su trans-

boxes) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible”, *Cuadernos de Derecho Privado*, n. 2, 2022, pp. 8-49 y “Análisis sobre las medidas de apoyo legal a la experimentación en tecnologías innovadoras”, *Revista Española de Derecho Aeronáutico y Espacial*, N.º 2 (Septiembre), 2022 (Ejemplar dedicado a: In memoriam excmo.sr.d. Rodolfo A. González-Lebrero), pp. 319-346.

⁷ OECD AI: “Investments in AI and data”, 2024, <https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-generative-ai-by-country>

⁸ Según parece, el concepto fue acuñado en 2012 por la profesora Anu Bradford de la *Columbia Law School*. En virtud del efecto Bruselas, las regulaciones de la UE se convierten en estándares globales.

Tanto este como el llamado efecto California -que se ciñe a la regulación en el ámbito medioambiental- entran dentro de esa “carrera hacia arriba” (“race to the top”) en la que las regulaciones más estrictas son más atractivas para las empresas porque teóricamente facilitan la producción y exportación. Justamente opuesto a dichos efectos, ciertos expertos en IA se refieren al efecto *Delaware*, una “carrera hacia abajo” en el que los países optan por rebajar sus requisitos regulatorios con un claro objetivo: atraer a empresas que buscan normas menos estrictas. Afirman que: “Ni uno ni otro se ha demostrado claramente, pero en el caso de la inteligencia artificial se ha reabierto el debate sobre una regulación demasiado estricta puede hacer que unos u otros acaban perdiendo la carrera por dominar esta tecnología”, Pastor, J. “La Unión Europea quiere dominar la revolución IA con regulación. Para los expertos es una mala idea”, Xataka, 13-12-2023, <https://www.xataka.com/robotica-e-ia/estallido-ia-se-ha-encontrado-viejo-enemigo-regulatorio-a-vuelta-esquina-efecto-bruselas>.

⁹ https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

¹⁰ El Producto Interior Bruto (PIB) en términos de Paridad de Poder Adquisitivo (PPA) es una medida económica que ajusta el PIB nominal de un país teniendo en cuenta las diferencias en el costo de vida y los niveles de precios entre países. La PPA se utiliza para comparar de manera más precisa el poder adquisitivo de los ciudadanos de diferentes países, ya que corrige las distorsiones que generan las fluctuaciones en los tipos de cambio y las disparidades de precios entre economías.

formación en productos comercializables, ya que las empresas innovadoras que buscan crecer en Europa se encuentran con obstáculos en cada fase motivados por la existencia de normativas que son restrictivas e inconsistentes.

Aunque no consideramos que se pueda hablar de la contraposición entre regulación *versus* innovación, la elaboración de legislación en un ámbito emergente, como es la IA, al igual que se ha planteado en materia de ciberseguridad o en el ámbito del RGPD¹¹, presenta algunos retos que han sido definidos mediante algunas teorías que nos parecen muy oportunas traer a colación. Se trata del “problema del ritmo” y el dilema de *Collingridge*¹². El “problema del ritmo” se refiere al desfase entre la introducción de nuevas tecnologías y la creación de leyes y mecanismos regulatorios que garanticen su desarrollo seguro. Mientras que la tecnología avanza rápidamente, la legislación y supervisión tienden a desarrollarse más lentamente. Aunque este ritmo más pausado en la legislación puede favorecer la estabilidad y exhaustividad, también deja a los usuarios desprotegidos. Se pone como ejemplo reciente la AIA, que debió ser modificada tras la aparición de ChatGPT, dado que su borrador inicial no contemplaba esta tecnología¹³. A pesar de que la IA generativa fue incorporada, algunos expertos consideran que el marco de riesgo/no riesgo de la ley es insuficiente para regular adecuadamente esta forma de IA. Este caso ilustra cómo los avances tecnológicos suelen ir más rápido que la evolución normativa.

Además, el “dilema de Collingridge” resalta los retos de regular nuevas tecnologías en diferentes fases de su desarrollo. En la fase inicial, hay poca información sobre los riesgos, lo que complica la creación de leyes adecuadas. En fases posteriores, cuando la tecnología ya está integrada en la sociedad, los costos de adaptar la normativa a esta realidad pueden ser elevados y el proceso lento¹⁴.

¹¹ O la edición del genoma humano o la nanotecnología, *vgr.*, WANG, L., et. al.: “Human genome editing after the “CRISPR babies”: The double-pacing problem and collaborative governance”, *Journal of Biosafety and Biosecurity*, 5(1), 2023, pp. 8-13.

¹² Seguimos para su explicación a BOEKEN, J.: “From compliance to security, responsibility beyond law”, *Computer Law & Security Review*, Volume 52, April 2024, 105926.

¹³ Como han advertido HELBERGER, N. /Diakopoulos, N.: “ChatGPT and the AI Act”, *Internet Policy Review* 12.1 (2023).

¹⁴ En su mensaje de veto al Proyecto de Ley SB-1047 sobre seguridad en IA, conocido como la *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*, que fue aprobado por la Asamblea legislativa de California en agosto de 2024, el Gobernador de California afirmó: “Quiero ser claro: estoy de acuerdo con los legisladores en que no podemos esperar a que ocurra una catástrofe para actuar y proteger al público. California no se retirará de su responsabilidad. Deben adoptarse protocolos de seguridad y medidas proactivas, con consecuencias claras y aplicables para aquellos que incumplan. Sin embargo, no creo que para proteger al público debamos conformarnos con una solución que no se base en un análisis empírico de la evolución de los sistemas y capacidades de IA. Un marco regulatorio efectivo debe evolucionar al ritmo de la tecnología misma”, BARRIOS, M.:

En este trabajo tratamos de aportar ciertas reflexiones y consideraciones en torno al nuevo panorama legislativo promulgado para regular, en la medida de lo conocido y por lo tanto viable, los sistemas de IA y el papel que la regulación sobre responsabilidad civil puede aportar para favorecer la competitividad e innovación en el marco europeo. En particular, nos centramos en la AIA y la futura Ley de Movilidad Sostenible, como ejemplo de legislación sectorial afectada por la IA, en cuanto impulsora de la experimentación para promover la innovación en materia de movilidad inteligente.

1.3. EL PROYECTO DE LEY DE MOVILIDAD SOSTENIBLE DE 23 DE FEBRERO DE 2024 CON RELACIÓN A LA APLICACIÓN DE LA IA EN VEHÍCULOS AUTOMATIZADOS

La Comisión Europea ha identificado la inteligencia artificial (IA) como clave para la automatización del transporte, apoyando pruebas de tecnologías emergentes a través del Programa Europa Digital, que destina fondos a la investigación y el desarrollo de IA en la movilidad. El Proyecto de Ley de Movilidad Sostenible de 23 de febrero de 2024 (en adelante, PLMS)¹⁵ establece las bases para regular la futura operación de vehículos automatizados, tanto de pasajeros como de mercancías, en vías públicas. Esta legislación busca, por un lado, adaptar la infraestructura legal y operativa a las nuevas tecnologías, y por otro, apoyar la innovación y asegurar que las pruebas se realicen de manera ordenada, segura y eficiente. Resalta el derecho a la movilidad como un derecho fundamental que las administraciones deben garantizar. Se promueve un sistema de movilidad eficiente y sostenible que no dependa del transporte privado motorizado, alineado con los Objetivos de Desarrollo Sostenible (ODS), como la reducción de las emisiones de gases de efecto invernadero, la infraestructura resiliente y la movilidad inclusiva.

En particular, el capítulo II del título V de la ley establece que, aunque la operación generalizada de estos vehículos aún no está permitida, las regulaciones actuales evolucionan constantemente. Cabe precisar que el PLMS no regula directamente el funcionamiento o la seguridad de los vehículos automatizados, sino que se enfoca en la promoción de su introducción gradual

“California no aprobará su Ley de innovación segura para modelos de inteligencia artificial de frontera”, fuente LinkedIn 5 de octubre de 2024.

Otro ejemplo que se aporta es el Metaverso, cuyo impacto completo y riesgos de seguridad son difíciles de predecir hasta que su adopción sea más generalizada. Adaptar la legislación a esta tecnología después de su implementación generalizada será complejo y costoso, al respecto, PEARLMAN, K., et. al.; “Securing the metaverse-virtual worlds need real governance”, *Simulation Interoperability Standards Organization-SISO*, 2023.

¹⁵ https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-9-1.PDF

mediante principios programáticos y procedimientos específicos para pruebas en carreteras¹⁶. Efectivamente, el capítulo II rubricado “vehículo automatizado”, comienza con una precisión legal de carácter programática aplicable a cualquier tipo de vehículo automatizado, tal como los denomina el PLMS. En función de ello, su alcance se despliega tanto sobre el espacio aéreo -de ahí que los drones se les califica de *aero-nave* (aunque también son “vehículos” en la acepción aportada por la RAE), como sobre los vehículos que discurran por carretera, vías (trenes) o agua (embarcaciones náuticas autónomas)¹⁷.

El PLMS otorga prioridad a estos vehículos automatizados para acceder a espacios controlados donde puedan realizar pruebas. Esto significa que los vehículos autónomos y los servicios de transporte que se presten con estos tendrán preferencia en áreas designadas para tal fin. Dichas áreas ofrecen un entorno seguro y supervisado para que se realicen experimentos y pruebas de funcionamiento en condiciones que minimicen riesgos tanto para los usuarios como para el entorno. Se advierte, desde el punto de vista de la seguridad (y añadimos también las cuestiones en torno a la responsabilidad, ya sea civil, sancionadora, penal o la propia patrimonial de la Administración), que cada tipología de vehículo cuenta con un marco regulatorio *sectorial*, tanto a nivel europeo como, en ocasiones, a nivel nacional, que *debe cumplirse imperativamente*¹⁸.

Con tal finalidad, entendemos, se recoge expresamente que “no es objeto de esta ley regular el funcionamiento de los vehículos ni sus condiciones de se-

¹⁶ Véase la Instrucción VEH 2022/07: Autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada y la web de la DGT para la solicitud de pruebas o ensayos de investigación, <https://www.dgt.es/nuestros-servicios/para-colaboradores-y-empresas/vehiculos-de-conduccion-automatizada/pruebas-o-ensayos-de-investigacion/>. Cabe señalar que la DGT ultima la normativa para regular la conducción automatizada, que se espera sea aprobada antes de finalizar 2024. Un resumen de la propuesta regulatoria ha sido resumida por DALMAU, J.: “La DGT ultima la normativa para la conducción autónoma”, *coches.net*, 6-2-2024, <https://www.coches.net/noticias/dgt-reglamento-conduccion-autonoma>. Entre la bibliografía más reciente, puede consultarse LAFUENTE SÁNCHEZ, R.: *Inteligencia artificial y vehículos autónomos: Responsabilidad civil extracontractual internacional*, Aranzadi, 2024.

¹⁷ Las referencias efectuadas al PLMS se han obtenido de nuestro trabajo “La responsabilidad civil en los espacios controlados de pruebas (regulatory sandboxes) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible”, *cit.*, n. 2, 2022, pp. 8-49. En el mismo, analizaba el Proyecto de Ley presentado en la anterior legislatura, cuyo contenido coincide con el presentado en el vigente periodo legislativo.

¹⁸ Aunque, en el seno de su articulado, art. 2.3 PLMS, segrega el concepto de “vehículo automatizado” para referirse a los vehículos a motor en vías públicas o de uso común referidos en el Cap. II del T. V. con rango de Ley, debería priorizarse el PLMS, en cuanto *lex specialis*, sin embargo, la legislación básica (*v.gr.* Ley 40/2015, de 1 de octubre, *de Régimen Jurídico del Sector Público*), así como el resto de leyes reguladoras de ciertos aspectos sobre seguridad o responsabilidad (en sus distintas vertientes), tendrán que aplicarse coordinadamente con esta futura Ley especial en materia de innovación.

guridad”⁸². De hecho, se declara en el art. 73 PLMS la responsabilidad exclusiva del promotor por el cumplimiento de lo contemplado en esta ley y *demás normativa aplicable*, en los términos recogidos en el protocolo de pruebas. Además, el informe de evaluación emitido por la autoridad de supervisión comprobará, entre otros aspectos, “el análisis del proyecto en el marco regulatorio”, art. 75.3.c) PLMS. Por todo ello, siempre encontrará cobertura en este contexto la regulación imperativa aplicable a cada medio de transporte, con independencia de que estamos hablando en términos de investigación e innovación en movilidad⁸³. Del engarce de la PLMS con la regulación de la AIA en ciertos aspectos, como el propio concepto de IA, nos ocupamos a lo largo de este trabajo, comenzando por abordar la dificultosa definición de sistema de IA.

1.4. EL CONCEPTO DE “SISTEMA DE INTELIGENCIA ARTIFICIAL” EN LA AIA Y PLMS

La propia definición de “sistema de IA” es una de las cuestiones de mayor dificultad y envergadura que rodean a esta tecnología disruptiva. La versión definitiva de AIA, declara que a los efectos del Reglamento, “se entenderá por «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales” (art. 3.1)¹⁹. Aunque esta definición se basa en la contemplada por la OCDE, peca de ser excesivamente amplia y genérica. Un reto importante será distinguir la IA del software tradicional, ya que no se exige un grado específico de autonomía, lo que dificulta la diferenciación entre ambos²⁰.

Efectivamente, conviene resaltar que con la definición de la AIA no se pretende abarcar sistemas de software o enfoques de programación tradicionales más sencillos. Al respecto, uno de los términos clave es el de “inferencia”, en la medida que se pretende que no incluya los sistemas basados en las normas definidas únicamente por personas físicas para ejecutar automática-

¹⁹ La influencia de la AIA es evidente en otros sectores donde se espera que la IA aporte grandes beneficios, como en el ámbito aeronáutico. Con relación a las definiciones de IA empleadas en este sector, véase . EASA (2023) “Artificial Intelligence Roadmap 2.0 A human-centric approach to AI in aviation”, <https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20>.

²⁰ Consagra en la legislación de la UE la definición acordada por la OCDE, en la medida que se ha pretendido armonizarla estrechamente con los trabajos de las organizaciones internacionales que se ocupan de la IA (declara el Considerando 12), Parlamento Briefing septiembre 24, p. 7.

mente operaciones. Como aclara el Considerando 12 AIA, una característica clave de los sistemas de inteligencia artificial es su habilidad para realizar inferencias. Esto implica la capacidad de generar resultados como predicciones, recomendaciones, decisiones o contenidos, que pueden impactar tanto en entornos físicos como virtuales. Además, los sistemas de IA son capaces de deducir modelos o algoritmos a partir de los datos o información de entrada. Las técnicas que hacen posible esta capacidad de inferencia incluyen enfoques de aprendizaje automático, donde el sistema aprende de los datos para alcanzar ciertos objetivos, así como estrategias basadas en la lógica y el conocimiento, que permiten inferir a partir de información codificada o representaciones simbólicas de la tarea a resolver. De este modo, la capacidad de inferencia de un sistema de IA va más allá del simple procesamiento de datos, al incorporar elementos de aprendizaje, razonamiento y modelado.²¹ El Considerando 12 del Acta de IA ofrece algunos matices, especificando que la autonomía implica cierta independencia en las acciones sin intervención humana, pero esto describe más bien la automatización que la autonomía real. Como se declara en el reciente *Complementary Impact Assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence* elaborado por Philip Hacker (en adelante, *Complementary Impact Assessment*)²², muchos dispositivos operan sin intervención humana, como cepillos de dientes eléctricos o máquinas de cocina, pero no se consideran IA, ya que no tienen capacidad de adaptación. La clave para diferenciar la IA radica en su capacidad para aprender a partir de datos que no ha visto antes, lo que está relacionado con el concepto de “inferencia” mencionado en el citado Considerando 12.

Este Considerando también excluye sistemas basados únicamente en reglas definidas por humanos, como las operaciones matemáticas básicas de

²¹ De este modo, los dos enfoques principales de la IA, el aprendizaje automático y los enfoques simbólicos o basados en el conocimiento, se engloban ahora bajo el concepto de “inferencia”. Esto resulta tranquilizador, aunque persisten ciertas lagunas, especialmente en relación con los sistemas simples basados en reglas o la modelización estadística. Aunque los considerandos no eliminan completamente la inseguridad jurídica, al menos aseguran que programas sencillos, como la función de autosuma en Excel, no se consideren IA. Esta función puede argumentarse que ha sido diseñada exclusivamente por humanos o que implica un procesamiento básico de datos. Si bien no existe una línea divisoria clara, los ejemplos que se piensan incluir en las directrices elaboradas por la Comisión, proporcionarán una ayuda considerable, se declara por parte del Parlamento Europeo, *Briefing* septiembre 24, p. 7.

²² European Parliamentary: *Complementary impact assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence*, Philip Hacker STUDY EPRS | Research Service Ex-Ante Impact Assessment Unit PE 762.861- September 2024, pp. 9 Y 10, quien remite para dicha diferenciación a W. Xu, ‘From automation to autonomy and autonomous vehicles: Challenges and opportunities for humancomputer interaction’, *Interactions*, Vol. 28(2), 2020, p. 50.

programas como Excel. Aunque la definición es amplia²³ y cubre tecnologías como los chatbots o sistemas avanzados de reconocimiento facial, plantea desafíos en su aplicación regulatoria, especialmente al diferenciar sistemas que deberían ser considerados IA y aquellos que no, como los sistemas basados en reglas y los modelos estadísticos avanzados que a veces pueden confundirse con IA.

Por su parte, en la Exposición de motivos del PLMS se afirma que: “La inteligencia artificial es un concepto que se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción (con cierto grado de autonomía) con el fin de alcanzar objetivos específicos. La utilización de la misma es cada vez más intensa en el ámbito del transporte y la movilidad”. Como nos parece obligado comparar este concepto con el aportado por el AIA, podemos destacar en primer término, la ambigüedad que implica hablar de “comportamiento inteligente” dado que no aclara qué se entiende por “inteligencia” en este contexto. La inteligencia es un concepto amplio y multifacético que varía según la disciplina (psicología, informática, filosofía, etc.), mientras que algunas habilidades sí se consideran indicativas de inteligencia en sistemas artificiales, como el aprendizaje, el razonamiento o la resolución de problemas. Igualmente cabe objetar que se haga referencia a que la acción cuente “con cierto grado de autonomía” pues se trata de una frase que peca claramente de generalidad al no establecer un umbral claro sobre cuánto es necesario para considerar a un sistema como IA. Además, todos los sistemas automatizados tienen algún nivel de autonomía, lo que podría generar confusión sobre dónde trazar la línea entre automatización y inteligencia artificial²⁴.

Por el contrario, entendemos que sí supone un claro acierto que el enfoque se limite al análisis del entorno y la acción física, pues el objeto de la futura LMS se centra en sistemas que interactúan físicamente con su ambiente²⁵. En consonancia la mención específica al transporte y movilidad queda justificada por el ámbito especial de la Ley, frente a las múltiples aplicaciones de

²³ El citado Considerando 12 AIA menciona los dos principales enfoques actuales de la IA: el aprendizaje automático y los enfoques basados en el conocimiento. Aunque esto hace poco por acotar más el concepto, el texto enfatiza que la capacidad de inferencia debe “trascender el procesamiento básico de datos” y permitir el “aprendizaje, razonamiento o modelado”. De ello se puede deducir que la IA, en el sentido de la ley, debe incluir algunas funciones adaptativas para abordar tareas más complejas, como predicciones intrincadas o la creación de contenido.

²⁴ Al respecto, puede consultarse el documento de JARUS para sistemas de aeronaves no tripuladas citado en la bibliografía y la conocida clasificación de SAE.

²⁵ Se excluyen de dicha definición sistemas de IA que operan en dominios virtuales o que no requieren interacción física, como motores de recomendación, algoritmos de detección de fraude o asistentes virtuales.

la IA que en la medida de su transversalidad, abarca también a otros sectores como la medicina, la educación, el comercio, entre otros.

2. DILEMAS EN TORNO A LA REGULACIÓN DE LA RESPONSABILIDAD CIVIL EN LAS ACTIVIDADES QUE EMPLEAN SISTEMAS DE IA

La responsabilidad civil se encuentra actualmente en una coyuntura crítica, tanto en la Unión Europea, como fuera de ella²⁶. Valga como ejemplo emblemático el reciente veto que ha sufrido el Proyecto de Ley SB-1047 sobre seguridad en IA, conocido como la *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act* y el enfoque más fragmentado, basado en iniciativas de autorregulación y parciales que viene imponiéndose en Estados Unidos²⁷. Varias cuestiones se encuentran sin resolver, no tanto por falta de interés del legislador comunitario sino por la dificultad de buscar el punto de equilibrio de los distintos intereses en juego y por las especiales características que imbrican los sistemas de IA, como pasamos a exponer. Si bien, reducir la incertidumbre es evidente que resultaría muy beneficioso para el sector empresarial, dado que estas organizaciones consideran que la responsabilidad por posibles daños (33%), la estandarización de datos (33%) y los obstáculos regulatorios (29%) son desafíos externos importantes para la adopción de IA²⁸.

²⁶ Como se declara en el *Complementary Impact Assessment* p I. Para una consulta de las principales legislaciones sobre IA a nivel global, puede consultarse MUÑOZ VELA, J.M.: *La regulación de la inteligencia artificial. Reto y oportunidad desde una perspectiva global e internacional*, Aranzadi, 2024.

²⁷ La legislación proponía introducir un régimen de responsabilidad objetiva (art. 22606(a) (5) SB 1047), según el cual los desarrolladores podrían ser considerados responsables de cualquier daño causado por sus sistemas de IA, incluso si han cumplido con todas las medidas de seguridad exigidas. Con este enfoque se persigue asegurar que los desarrolladores adopten todas las precauciones necesarias para evitar consecuencias imprevistas y reducir los riesgos asociados con el uso de tecnologías de IA avanzadas. Respecto al comentario de esta Propuesta legislativa, nos remitimos *Complementary Impact Assessment* I H P 2. Sobre el motivo del veto, puede leerse a BARRIOS, M.: “California no aprobará su Ley de innovación segura para modelos de inteligencia artificial de frontera”, fuente LinkedIn 5 de octubre de 2024

²⁸ Al analizar los obstáculos para la adopción de IA en empresas de diferentes tamaños, se observa una mayor variación, especialmente al comparar grandes empresas (con 250 o más empleados) con micro, pequeñas y medianas empresas. Un ejemplo claro es que el 40% de las grandes empresas consideran que las estrictas normativas para el intercambio de datos, como las leyes de protección de datos, representan un obstáculo importante, mientras que esta cifra es del 33% cuando se consideran empresas de todos los tamaños combinados. Además, un 33% de las grandes empresas identifica la falta de acceso a datos privados de alta calidad como un desafío significativo para la adopción de IA, en comparación con solo el 26% de las empresas más pequeñas. Por otro lado, las micro, pequeñas y medianas empresas son más propensas a percibir la falta de financiación pública o externa como una barrera importante (37% en promedio), en contraste con las grandes empresas (32%).

2.1. CARACTERÍSTICAS ESPECIALES DE LOS SISTEMAS DE IA CON RELACIÓN AL RIESGO

Los principios de “no hacer daño de los métodos de IA”, que no se infrinjan los valores fundamentales que rodean a la persona y se tenga como objetivo siempre la determinación humana final, ya formaba parte de la Recomendación de la UNESCO *sobre la ética de la inteligencia artificial* en 2021²⁹. Y es que el nivel aceptable de riesgo para las personas, los bienes personales o a las infraestructuras críticas derivado de la introducción de una tecnología de IA, se considera que no debe ser superior al de un sistema tradicional equivalente³⁰. Aunque ello no podrá impedir que disminuya la confianza de los ciudadanos ante la probabilidad de que el nivel de compensación establecido por las normativas nacionales sobre responsabilidad civil pueda ser inferior en comparación con aquellos casos donde las tecnologías involucradas en la causación del daño no están relacionadas con la IA. Estas disparidades en la indemnización podrían afectar negativamente la aceptación social de la IA y minar la confianza en los productos y servicios que la emplean (Considerando 4 PDRCIA)³¹.

No obstante, a medida que esta tecnología incrementa su automatización y, por consiguiente, su grado de autonomía, no se observa, a nuestro entender, un aumento en el número de accidentes o daños, basándonos en los últimos

En cuanto a las diferencias sectoriales, aunque las variaciones en los obstáculos externos para la adopción de IA son limitadas, algunos ámbitos destacan en ciertos desafíos. La falta de financiación pública o externa es vista como un obstáculo significativo en sectores como el trabajo social (51%), educación (45%), alimentación (43%) y salud humana (41%). En cambio, sectores como el petróleo y gas (21%), transporte (31%), finanzas y seguros (31%), y servicios de recreación (32%) son menos propensos a ver la falta de financiación como un obstáculo importante. Estos sectores tienden a mostrar más preocupación por las estrictas normas de intercambio de datos, especialmente en petróleo y gas (41%), finanzas y seguros (40%), y salud humana (40%), lo que refleja una variación en las prioridades según la actividad económica, European Commission: Directorate-General for Communications Networks, Content and Technology, *European enterprise survey on the use of technologies based on artificial intelligence - Final report*, Publications Office, 2020, <https://data.europa.eu/doi/10.2759/759368>, pp. 58-60.

²⁹ Así como desde el perfil de la ciberseguridad, los daños no deseados, como los riesgos de seguridad y las vulnerabilidades a los ataques, deben evitarse y abordarse durante todo el ciclo de vida de los sistemas de IA. UNESCO C. *Recommendation on the ethics of artificial intelligence* (2020) Digital Library UNESDOC, URL en.unesco.org, comentada por N. DÍAZ-RODRÍGUEZ et al. “Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation Information Fusion Volume 99, November 2023, 101896

³⁰ EASA, *Op. cit.* p. 30.

³¹ Cuestión también advertida en European Commission: Directorate-General for Justice and Consumers, Mosoreanu, M., Ulicna, D., Paetz, S., Podobea, V. et al., *Behavioural study on the link between challenges of artificial intelligence for Member States' civil liability rules and consumer attitudes towards AI-enabled products and services - Final report*, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2838/24993>

datos sobre siniestralidad al efecto³². Un estudio ha analizado la seguridad de los vehículos autónomos en comparación con los operados por personas. La investigación revisó datos de 2.100 accidentes protagonizados por vehículos autónomos y más de 35.000 incidentes ocurridos con vehículos controlados por humanos, entre 2016 y 2022, principalmente en California (Estados Unidos). Las conclusiones del estudio indican que los vehículos autónomos son más seguros en muchas situaciones de conducción, aunque presentan una mayor incidencia de accidentes en momentos específicos, como durante maniobras de giro o en condiciones de luz limitada, como el amanecer y el atardecer³³. Por ello, no puede calificarse la IA, de manera anticipada, como una actividad anormalmente peligrosa que deba estar sujeta a un criterio de responsabilidad objetiva, además de por otros argumentos que aduciremos más adelante³⁴.

En la versión definitiva de la AIA (arts. 5 y 6), los sistemas de IA pueden llegar a clasificarse de “prácticas prohibidas”, como de alto riesgo. Bajo esta segunda hipótesis, se concreta que el sistema de IA adquirirá dicha categoría en estos dos casos: cuando están integrados como componentes de seguridad en productos cubiertos por la legislación vigente sobre productos, como se menciona en el anexo I, o cuando constituyen en sí mismos dichos productos, como podría ser el caso de software médico basado en IA o incluido en jugue-

³² Los niveles de automatización de los vehículos siguen, comúnmente, la clasificación elaborada, en 2014 por la Sociedad de Ingenieros de Automoción Internacional (SAE por su acrónimo en inglés, *Society of Automotive Engineers*), y van desde la ausencia de automatización (nivel 0) hasta la automatización completa (nivel 5). Para la clasificación se tiene en cuenta sobre todo el papel del ocupante del vehículo, más que lo que éste es capaz de hacer o de no hacer. De ese modo, en los niveles 0 a 2, que son los más bajos en automatización, el conductor debe realizar prácticamente la mayor parte de las tareas que lleva consigo la conducción, y sólo es a partir del nivel 3 (automatización condicional), cuando su papel se hace más pasivo y el sistema ya toma algunas decisiones de manera continuada, tras monitorizar el entorno; en el nivel 4 (automatización alta), el papel del conductor en ocasiones puede llegar a desaparecer: así sucede cuando concurren determinadas circunstancias geográficas (barrios específicos, como los residenciales, escolares, militares) o ambientales (condiciones meteorológicas o diurnas/nocturnas); no obstante, el conductor puede desactivar el sistema y conducir él en cualquier momento; y, por último, en el nivel 5 (automatización total) el ocupante es un simple pasajero y el vehículo es autónomo en cualquier circunstancia, explica ATIENZA NAVARRO, M.L.: *Op. cit.*, p. 350.

³³ Los resultados se publican en la revista *Nature Communications* SMC España, 18/06/2024, <https://sciencemediacentre.es/un-estudio-compara-la-seguridad-de-los-vehiculos-autonomos-frente-los-conducidos-por-personas>.

³⁴ Marchisio, “In support of ‘no-fault’ civil liability rules for artificial intelligence” (2021) 1 SN Social <https://doi.org/10.1017/err.2021.52>, publicado en línea por Cambridge University Sciences. Al respecto, art. 5:101 Principios de Derecho europeo de la responsabilidad civil, dispone que, cuando se trate de actividades anormalmente peligrosas, la persona que las lleva a cabo responde objetivamente de los daños, con lo que en este supuesto no haría falta culpa alguna por parte de los dependientes, disponible en <http://www.egtl.org/docs/PETLSpanish.pdf>.

tes, aviación, automóviles, y ascensores³⁵. A su vez, se califican casos de uso de alto riesgo los enumerados en el anexo III de la Ley de IA. Esta lista incluye situaciones en las que el uso de la IA es particularmente sensible, especificando casos concretos en ámbitos como la educación, el empleo, la aplicación de la ley o la migración. Asimismo, se hace referencia a sistemas de IA utilizados como componentes de seguridad en infraestructuras digitales críticas, el tráfico rodado y el suministro de agua, gas, calefacción y electricidad³⁶.

Sin embargo, como puede observarse, conforme a la clasificación actual de los niveles de riesgo, se ha eliminado la referencia a los vehículos autónomos que, por el contrario, se aboga por volver a incorporarla en el *Complementary Impact Assessment* publicado recientemente³⁷. En concreto, se justifica que el enfoque de la AIA en determinados casos de uso de alto riesgo -como la identificación biométrica, el reconocimiento de emociones, el empleo, la calificación crediticia, y los seguros de salud y vida- no cubre el espectro completo de aplicaciones de IA que podrían generar importantes riesgos de responsabilidad. Es por ello, que se plantea sustituir la denominación “alto riesgo”, por “alto impacto”, como se ha propuesto en Canadá³⁸, para dar así entrada a aplicaciones de IA adicionales como los vehículos autónomos (o la IA relacionada con el transporte) y modelos de seguros más amplios, que no están incluidas en las categorías de alto riesgo según la Ley de IA, demostrándose que el potencial de daño puede superar las clasificaciones actualmente prescritas³⁹. Recordemos que en la versión previa de la Propuesta última conocida de Reglamento de 2020, se calificaban “de alto riesgo” los siguientes sistemas de IA: 1) aeronaves no tripuladas (UAS) según el artículo 3, punto 30, del Reglamento (UE) 2018/1139, es decir, drones que operan o están diseñados para operar de forma autónoma o bajo control remoto sin piloto a bordo (en el sector del transporte); 2) vehículos con niveles de automatización 4 y 5, de acuerdo con la norma SAE J3016 (en el sector del transporte); 3) sistemas autónomos de gestión del tráfico (en el sector del transporte); 4) robots autónomos (en el sector asistencial); y 5) dispositivos autónomos para la limpieza de espacios públicos (en el sector asistencial).

³⁵ Como especifica el Considerando 50. Por su parte, la Comisión está preparando directrices para la clasificación de alto riesgo, que se publicarán antes de la fecha de aplicación de estas normas.

³⁶ Sobre la aplicación de U-Space, puede consultarse Bustos Moreno, Y.: “The Implementation of U-space: Open Challenges from the Legal-Private Perspective”, Pastor Sempere, C. (Ed.). *Legal Framework for New Digital Assets, Identities and Data Space: Governance and Control of Data and Digital Economy in the European Single Market* [Subt. & Tit.]. Springer Cham. (Law, Governance and Technology Series; 16).

³⁷ *Complementary Impact Assessment*, pp. 14-15-16.

³⁸ Sistema que *infra* exponemos en el texto principal.

³⁹ El citado estudio *Complementary Impact Assessment* propone que la PDRCIA amplíe su ámbito de aplicación para incluir los sistemas de propósito general y otros “sistemas de IA de alto impacto”, así como los programas informáticos.

Por lo tanto, el actual enfoque para clasificar los sistemas de IA de alto riesgo conforme a la Ley de IA podría no ser completamente adecuado para un marco de responsabilidad por IA, según se ha afirmado en el *Complementary Impact Assessment*⁴⁰. Esto se debe a que se considera que la AIA se centra principalmente en riesgos a nivel social, sin considerar adecuadamente las variaciones en la exposición al riesgo individual. Por ejemplo, se expone que un escenario en el que un pequeño grupo de personas dentro de una población más amplia sufra daños significativos debido a un sistema de IA, podría no cumplir con el umbral necesario para ser clasificado como de alto riesgo bajo la Ley de IA. Sin embargo, desde una perspectiva de responsabilidad civil, el impacto sobre estas personas subraya la necesidad de un enfoque más matizado que reconozca tanto los riesgos sociales como los individuales⁴¹.

Una de las propuestas más similares a la Ley de IA es la Ley de Inteligencia Artificial y Datos (AIDA) de Canadá, presentada como parte del proyecto de ley C-27, que busca regular la IA en el país⁴². Al igual que la Ley de IA, AIDA adopta un enfoque basado en el riesgo, enfocándose en los “sistemas de IA de alto impacto”, es decir, aquellos con el potencial de causar daños significativos o afectar la seguridad pública. Según AIDA, las organizaciones que desarrollen o utilicen estos sistemas deberán realizar evaluaciones de riesgos, implementar estrategias de mitigación y supervisar continuamente sus sistemas para asegurar que cumplen con los estándares de seguridad y ética establecidos.

En cuanto a la responsabilidad, AIDA pone el énfasis en que las entidades sean responsables por los daños ocasionados por sus sistemas de IA. No obstante, la aplicación de la ley se basa en la supervisión pública en lugar de en litigios privados (art. 29-30 y 40 AIDA). Esto incluye la imposición de multas significativas por incumplimientos negligentes (art. 30(4) AIDA) y otor-

⁴⁰ En septiembre de 2022, la Comisión Europea presentó una propuesta de Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (PDRCIA), acompañada de una evaluación de impacto. La Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo solicitó la presente evaluación de impacto complementaria de la propuesta, que se centra en cuestiones de específicas de investigación, European Commission, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, SWD(2021) 168 final, 2021.

⁴¹ *Complementary Impact Assessment* siguiendo a M. C. Buiten, A. De Streel y M. Peitz, “The law and economics of AI liability”, *Computer Law & Security Review*, Vol. 48, Artículo 105794, 2023, p. 18; J. De Bruyne, O. Dheu y C. Ducuing, “The European Commission’s approach to extra-contractual liability and AI - An evaluation of the AI liability directive and the revised product liability directive”, *Computer Law & Security Review*, Vol. 51, artículo 105894, 2023, p. 4 (ambos sobre vehículos autónomos); P. Hacker, “The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future”, *Computer Law & Security Review*, artículo 105871, Vol. 51, 2023, pp. 9-10.

⁴² Expuesta en el *Complementary Impact Assessment*.

ga al Comisario de IA y Datos la facultad de supervisar y hacer cumplir esta regulación⁴³.

Otra cuestión que invita a reflexionar sobre el régimen sustantivo armonizado, aún indefinido de la responsabilidad civil, que opera principalmente bajo criterios de imputación subjetiva en la mayoría de las legislaciones nacionales, es el que advierte Rubí⁴⁴ y que el derecho de daños deberá abordar. En primer lugar, se plantea si la falta de adopción de una tecnología más segura debe considerarse siempre negligente o si es aceptable seguir utilizando una tecnología menos segura sin incurrir en responsabilidad civil (principio de *grandfathering*). En este análisis, también será necesario determinar el nivel de esfuerzo y la inversión económica requeridos para que una decisión privada sea considerada diligente. Esto incluye la duda sobre si sólo se exige la adopción del estándar tecnológico común en el sector o si, por el contrario, se debe implantar la mejor tecnología disponible en términos de seguridad (*Best Available Technology* - BAT). Y es que, como hemos expuesto, uno de los problemas de base a los que se enfrenta la UE es la necesidad de inversión. El verdadero desafío radica en la vacilación para adoptar tecnologías de IA que, aunque podrían ofrecer importantes beneficios a usuarios, consumidores, trabajadores y al público en general, también implican nuevos gastos que las empresas tendrían que asumir, gastos que los beneficiarios no están dispuestos a cubrir⁴⁵. A ello se unen las exhaustivas obligaciones a cumplir, conforme dispone la AIA, particularmente para los sistemas de IA de alto riesgo, si bien no serán aplicables hasta dentro de tres años, en concreto, a partir del 2 de agosto de 2027⁴⁶.

Y es que debemos ser conscientes de las especiales características que acompañan a esta tecnología, en virtud de la cual se vienen identificando varios problemas derivados del desarrollo y uso de los sistemas de IA. De forma sistemática, el Parlamento Europeo ha enunciado la (i) opacidad (capacidad limitada de la mente humana para comprender cómo operan ciertos sistemas de IA), (ii) complejidad, (iii) adaptación continua e imprevisibilidad, (iv) comportamiento autónomo, y (v) dependencia funcional de los datos y

⁴³ Parlamento de Canadá, “An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Act”, proyecto de ley C-27.

⁴⁴ RUBÍ PUIG, A.: “Retos de la inteligencia artificial y adaptabilidad del derecho de daños”, *Retos jurídicos de la inteligencia artificial*, coord.. Cerrillo i Martínez, A./ Peguera Poch, M., pp. 62-63.

⁴⁵ Como han expuesto ALEXANDER, C. et al.: “Safer not to know? Shaping liability law and policy to incentivize adoption of predictive AI technologies in the food system”, *Front. Artif. Intell.*, 2023, pp. 4-5.

⁴⁶ El art. 113 AIA dispone que el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

de su calidad⁴⁷. En particular, nos interesa centrarnos en dos rasgos⁴⁸. La naturaleza abierta de los sistemas inteligentes implica que no operan como sistemas cerrados e inmutables, sino que están sujetos a actualizaciones y mejoras continuas. Muchas de estas mejoras surgen a través de la interacción con otros sistemas o fuentes de datos, e incluso pueden ser implementadas por terceros. A diferencia de los productos tradicionales, estos sistemas permanecen “abiertos” una vez que se lanzan al mercado. Gracias a su capacidad de autoaprendizaje y autonomía⁴⁹, los sistemas inteligentes pueden aprender de la experiencia y modificar su comportamiento en función de los datos que reciben, adoptando decisiones de manera completamente independiente, y en ocasiones, de forma que resulta inexplicable para sus propios creadores. Esta autonomía y capacidad de autoaprendizaje generan, desde una perspectiva legal, una completa “imprevisibilidad” respecto a las decisiones que toman los sistemas inteligentes⁵⁰, y una “desvinculación” de la supervisión humana, lo que plantea importantes desafíos en cuanto a la determinación de la responsabilidad por los daños causados y problemas de causalidad⁵¹. Por todo ello, considera Atienza que estas características son las más disruptivas en el ámbito de la responsabilidad y la inteligencia artificial y complican la aplicación de los esquemas monocausalistas y antropocéntricos de las reglas tradicionales de la responsabilidad civil⁵².

⁴⁷ Tras la amplia consulta pública que lanzó la Comisión europea en 2020, publicando una Evaluación de Impacto del Reglamento sobre Inteligencia Artificial, un estudio de apoyo y una propuesta preliminar, que recibieron comentarios de las partes interesadas.

⁴⁸ Como afirma ATIENZA NAVARRO, estas características han sido analizadas en muchos estudios realizados en el ámbito europeo, *op. cit.*. Por todos, pueden verse los elaborados por el *European Law Institute (ELI)*: Karner, E., et al.: *Comparative law study on civil liability for artificial intelligence*, estudio encargado por la Comisión Europea, Dirección General de Justicia y Consumidores al *European Law Institute (ELI)*, 2021 (disponible en <https://data.europa.eu/doi/10.2838/66412>), p. 15; Koch, B. et al., *Response of the European Law Institute (ELI) to the Public Consultation of the European Commission on Civil Liability Adapting liability rules to the digital age and artificial*, 10 enero 2022, pp. 23 a 27 (disponible en *intelligencelaw* https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_Public_Consultation_on_Civil_Liability.pdf Instituto de Derecho Europeo).

⁴⁹ A esta propiedad a la que se hace referencia en la propia definición al referirse a la “capacidad de adaptación” que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso, Considerando 12 AIA.

⁵⁰ Los posibles agentes responsables no pueden prever el comportamiento de los algoritmos de IA, en los que intervienen diversas variables, como las bases de datos, la recopilación de big data y la actuación de los propios usuarios finales, MARCHISIO, *Op. cit.*, p. 54.

⁵¹ Sobre esta problemática EVANGELIO LLORCA, R.: “Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE”, *Derecho de Contratos, Responsabilidad Extracontractual e Inteligencia Artificial*, APPDC, coord.. N. Álvarez Lata, pp. 559-633.

⁵² ATIENZA NAVARRO, M.L.: “La responsabilidad civil por daños causados por inteligencia artificial. estado de la cuestión”, *Derecho de Contratos, Responsabilidad Extracontractual e Inteligencia Artificial*, APPDC, coord.. N. Álvarez Lata, siguiendo a PALMERINI, E., «Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea», *Revista de Derecho Privado*,

No obstante, siguiendo la exposición de dicha autora⁵³, no pueden dejarse al margen los *deberes de actualización* de los operadores económicos que implementan sistemas inteligentes y su vinculación con los riesgos del desarrollo. La jurisprudencia del TJUE⁵⁴ ha tratado de interpretar esta causa de exoneración “objetivándola” (al margen de la diligencia exigible) al aplicar la responsabilidad por productos defectuosos, pero sigue generando controversia al introducir elementos subjetivos, ya que evaluar si el defecto era detectable según el estado de la ciencia y técnica implica valorar la diligencia del productor. En el caso de la inteligencia artificial fuerte, esta exoneración podría hacer ineficaz la responsabilidad de los operadores, dado que los sistemas con autoaprendizaje pueden generar daños que no se podían prever cuando fueron introducidos en el mercado. Esta preocupación ha llevado a algunos autores y documentos de la UE a pedir la eliminación de esta cláusula, al menos para la IA. En la versión última de la Directiva de Responsabilidad por Productos Defectuosos (DRPD)⁵⁵ el art. 18.1 determina que, como excepción a la exoneración basada en los riesgos de desarrollo: “1. Como excepción a lo dispuesto en el artículo 11, apartado 1, letra e),⁵⁶ los Estados miembros podrán mantener en sus sistemas jurídicos las medidas vigentes por las que los operadores económicos sean responsables aunque demuestren que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado o puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso”.

Universidad Externado de Colombia, n° 32, enero-junio 2017, pp. 53 a 97 (traducción al castellano de DÍAZ LINDAO, I.), p. 76.

⁵³ *Ibid*, pp. 403-404.

⁵⁴ STJCE 29 de mayo de 1997, ur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61995CJ0300&from=EN.

⁵⁵ Esta Directiva ha sido aprobada el 12 de marzo de 2024. P9_TA (2024)0132 Responsabilidad por los daños causados por productos defectuosos Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM(2022)0495 - C9-0322/2022 - 2022/0302(COD)). Para un recorrido de todo el proceso prelegislativo y de la situación anterior, puede consultarse MARÍN SALMERÓN, A.: *El defecto de diseño en los productos digitales*, Aranzadi, 2023, y del mismo autor: “Algunas reflexiones sobre las propuestas de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos, Contratación en el entorno digital”, coord. por I. González Pacanowska, M. C. Plana Arnaldos, 2023, pp. 391-462.

⁵⁶ Art. 11 DRPD: “Exención de responsabilidad. 1. Los operadores económicos a que se refiere el artículo 8 no serán responsables de los daños causados por un producto defectuoso si demuestran que: e) que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso.

2.2. EL DEBATE SOBRE EL RÉGIMEN DE RESPONSABILIDAD CIVIL MÁS FAVORABLE A LA INNOVACIÓN EN SISTEMAS DE IA

Como ya hemos expuesto, uno de los factores que se atribuyen a la falta de competitividad en Europa viene de la mano de una excesiva regulación de normas a nivel preventivo, que son básicamente las previstas en la AIA. Además, cabe plantear aquí otro de los posibles ingredientes, que sería introducir reglas de responsabilidad civil demasiado restrictivas o “opresivas” para quienes invierten en este sector⁵⁷.

El debate tiene como punto de partida la disyuntiva de la adopción de un régimen de responsabilidad objetiva para los sistemas de IA (o solamente para los de alto riesgo, como ya propuso la Propuesta de Reglamento de 2020), o bien respetar el criterio de imputación subjetiva preponderante en los países miembros (responsabilidad civil extracontractual basada en la culpa), *ex art.* 2.5 y Exposición de motivos, ap. 5 PDRCIA. No así en el ámbito del transporte que, además, es excluido del PDRCIA, art. 1.3.a).

La responsabilidad estricta transfiere el coste del conocimiento y control del riesgo del usuario a aquellos sujetos que se consideran responsables del riesgo, como los productores y operadores. De acuerdo con el principio de internalización de los gastos, que establece que quienes se benefician de una actividad riesgosa también deben asumir las consecuencias económicas asociadas, la responsabilidad objetiva asegura que quienes obtienen beneficios de las tecnologías de IA sean responsables de compensar los daños que estas puedan ocasionar. Esta completa internalización de las externalidades está alineada con los principios de justicia económica y distributiva (*qui habet commoda ferre debet onera*)⁵⁸.

Esto provocará un aumento considerable en las inversiones que posibiliten el cumplimiento, desarrollo y responsabilidad para estos actores, afectando especialmente a las pequeñas y medianas empresas (pymes), que pueden verse incapacitadas de asumir estos costes en un régimen de responsabilidad estricta⁵⁹. Las pymes ya se enfrentan una desventaja significativa, en la medida que los recursos en IA están concentrados en unas pocas grandes empresas. Debido a la falta de fondos suficientes, es probable que estas pequeñas corporaciones se mantengan alejadas del desarrollo de IA, considerando que los costes asociados al cumplimiento de las normativas sobre responsabilidad en

⁵⁷ Como ya advirtió ALPA, senza reprimere lo sviluppo economico “Quale modello normativo europeo per l’intelligenza artificiale?”, *Contratto e impresa*, 4/2021,, p. 1019.

⁵⁸ *Complementary Impact Assessment*.

⁵⁹ TRUBY, J. et al.: “A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications” *European Journal of Risk Regulation* (2022), 13, p. 292, doi:10.1017/err.2021.52

IA representan alrededor del 17% de la inversión total en esta tecnología⁶⁰. Para las pymes, este porcentaje podría ser aún mayor debido a la falta de economías de escala. En este sentido, se considera que este tipo de responsabilidad objetiva podría fomentar monopolios en la industria de IA, lo que supondría un riesgo para los consumidores, que acabarían asumiendo los costes, ya que se les transferiría ese impacto económico⁶¹.

Si bien se podría argumentar que los seguros podrían mitigar los costes regulatorios de la responsabilidad objetiva en IA para las pequeñas empresas, es poco probable que cubran todos los riesgos, especialmente aquellos que son incontrolables e imprevisibles. Además, esta garantía no resolvería el problema de la limitación de la innovación, ya que, aunque podría mejorar la tolerancia al riesgo, no incentivaría necesariamente la experimentación y el desarrollo de nuevas tecnologías⁶². Ante esta situación, la participación en entornos de “sandbox” regulatorio se plantea como una salida beneficiosa para las pymes y la propia innovación, como explicamos *supra*.

En el *Impact Assessment* de la Comisión Europea que acompañó la PDRCIA se valoraron tres opciones de política legislativa⁶³. La primera simplemente preveía regular medidas para aliviar la carga de la prueba que recae sobre las víctimas que intentan presentar pruebas que apoyen su demanda de responsabilidad civil. La otra vía establecía dichas estrategias (opción primera), pero añadiendo la armonización de las normas de responsabilidad objetiva en los casos de uso de IA con un perfil de riesgo particular, unido a la exigencia de un seguro obligatorio. Finalmente, se decidió acometer en una primera fase ciertos mecanismos procesales a favor de las partes demandantes⁶⁴, estipulando un mecanismo de *revisión*⁶⁵ para reevaluar, en particular, la necesidad de armonizar la responsabilidad objetiva en los casos de uso de IA con un perfil de riesgo particular (posiblemente acompañado de un seguro obligatorio)⁶⁶.

⁶⁰ RENDA *et al.*, p. 166.

⁶¹ BATHAEE, Y. *Op. cit.*, p. 930

⁶² TRUBY, J. *et al.*: *Op. cit.*, p. 292.

⁶³ European Commission, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, SWD(2021) 168 final, 2021.

⁶⁴ En consonancia con su política de «legislar mejor», la Comisión sometió la presente propuesta a una evaluación de impacto que fue examinada por su Comité de Control Reglamentario. La reunión del Comité de Control Reglamentario del 6 de abril de 2022 dio lugar a un dictamen favorable con observaciones, donde se decidió optar por la tercera vía. Como se explica en la Exposición de Motivos de la PDRCIA, p. 9.

⁶⁵ Con relación al AIA, véase el art. 112 AIA:

⁶⁶ Se ha puesto en marcha un programa de seguimiento para proporcionar a la Comisión información sobre incidentes relacionados con sistemas de IA. La revisión específica evaluará si serían

2.3. EL REPLANTEAMIENTO DE LA RESPONSABILIDAD OBJETIVA EN EL *COMPLEMENTARY IMPACT ASSESSMENT*. *PROPOSAL FOR A DIRECTIVE ON ADAPTING NON-CONTRACTUAL CIVIL LIABILITY RULES TO ARTIFICIAL INTELLIGENCE*

En la actualidad ha cobrado, si cabe, más fuerza el debate en torno al establecimiento de un régimen de responsabilidad sin culpa aplicable a sistemas de IA. Por nuestra parte, también nos planteamos si resulta tan perjudicial la imposición de la responsabilidad objetiva para respaldar la innovación tras el análisis del *Complementary Impact Assessment* publicado en septiembre de 2024. En este trascendente Estudio, se considera que una evaluación superficial de las desventajas de la responsabilidad estricta limita la capacidad de comparar adecuadamente las implicaciones de las distintas opciones regulatorias, obstaculizando la identificación del marco más efectivo y eficiente para la responsabilidad en IA. Recordemos que este régimen sin culpa viene rigiendo las actividades calificadas tradicionalmente como de mayor riesgo⁶⁷.

Una de las principales críticas a la implementación de la responsabilidad estricta en la regulación de la IA es la supuesta falta de certeza jurídica debido al perfil de riesgo incierto y al desarrollo continuo de esta tecnología disruptiva. Sin embargo, este argumento parece discutible, desde el momento que el AIA se ha enfrentado a problemas similares al definir las categorías de riesgo, lo que no ha impedido su amplia regulación⁶⁸. Además, se aduce en el citado Estudio de Hacker que las categorías de riesgo pueden ajustarse fácilmente mediante actos delegados o de implementación en la PDRCIA, como se prevé en la AIA. La certeza jurídica no depende solo de las categorías de riesgo, sino que la responsabilidad estricta ofrece mayor claridad que los regímenes basados en la culpa, al no requerir la definición de estándares específicos para los deberes de cuidado. Contrariamente a lo que se sugiere, la responsabilidad estricta podría proporcionar más seguridad legal al elimi-

necesarias medidas adicionales, como la introducción de un régimen de responsabilidad objetiva o un seguro obligatorio. Es necesario prever una revisión de la presente Directiva [cinco años] después de la finalización del período de transposición. En particular, mediante dicha revisión debe examinarse si es necesario adoptar normas de responsabilidad objetiva (sin culpa) para las demandas contra el operador -siempre que estas no estén ya cubiertas por otras normas de responsabilidad de la Unión, en particular la Directiva 85/374/CEE- combinadas con un seguro obligatorio para la explotación de determinados sistemas de IA, tal como ha sugerido el Parlamento Europeo (Considerando 31 y art. 5 PDRCIA).

⁶⁷ Al respecto, E. KARNER, et al.: *op. cit.*, 2021, p. 58.

⁶⁸ En un reciente estudio publicado por KPMG (Trusted AI governance) se describen los principales riesgos específicos que plantea la IA. Puede consultarse en https://media.lidn.com/dms/document/media/D4D1FAQGNtYPp0gfr1g/feedshare-document-pdf-analyze-d/0/1728371213794?e=1729123200&v=beta&t=01_EQFBxCBnx8v-UgyLRCi2bb2TONVQk_ooJQ-q5X3sQ p. 5.

nar la necesidad de establecer culpa⁶⁹. La responsabilidad estricta también podría cubrir vacíos dejados por los regímenes procesales, ya que no sería necesario depender de informes de expertos costosos para probar la culpa y facilitaría los procedimientos judiciales, al requerir solo la prueba de que un daño fue causado por una IA. Al mismo tiempo, el papel de las aseguradoras beneficiaría a las víctimas, ayudando a garantizar la compensación, como ocurre en el sector automotriz.

Otra objeción del *Complementary Impact Assessment* radica en razonar que un régimen de responsabilidad estricta para IA de alto riesgo podría ir más allá de los productos no relacionados con IA. Sin embargo, se podría haber considerado armonizar el derecho de responsabilidad civil entre los Estados Miembros, introduciendo disposiciones de responsabilidad estricta para productos de alto riesgo, no limitándose solo a la IA.

Además, no explora en detalle la posibilidad de combinar la responsabilidad objetiva con límites indemnizatorios⁷⁰, pese a los importantes efectos adversos que la de carácter ilimitado podría tener para la industria y el comercio en general⁷¹, a diferencia de la previsión de la Resolución del Parlamento europeo de 2020⁷². Ello resulta realmente importante para mantener la asegurabilidad que debería exigirse en los sistemas de IA, al menos, en los de alto riesgo, como se considera la conducción autónoma o la IA aplicada al diagnóstico médico⁷³.

⁶⁹ Como se reconoce en el estudio económico de Deloitte, “Study to support the Commission’s impact assessment on liability for artificial intelligence” European Commission, July 2021.

⁷⁰ Esta omisión es uno de los principales puntos débiles de la *Impact Assessment*, se afirma en este último Estudio de septiembre de 2024. DÍAZ ALABART también se mostró a favor de introducir límites indemnizatorios al modo en que ya se había efectuado en la Directiva 85/374 sobre productos defectuosos, *Robots y Responsabilidad Civil*, 2018, Reus, p. 62.

⁷¹ Con relación a EEUU, Alexander analiza los efectos beneficiosos y perjudiciales con relación a los posibles sujetos responsables y las víctimas. Termina concluyendo que el *statu quo* de la responsabilidad limitada se tolera porque no se ha encontrado una alternativa aceptable. La opción de la responsabilidad ilimitada se considera inaceptable porque el efecto potencialmente adverso sobre el comercio sería demasiado grande, incluso con una norma de responsabilidad personal proporcionada, *op. cit.*, p. 5.

⁷² En concreto, esta Propuesta sugería un tope de 2 millones de euros por daños personales y de 1 millón de euros por daños materiales (artículo 5 de la Resolución del Parlamento Europeo de 2020 sobre la responsabilidad de AI). La resolución también pide un seguro obligatorio para estos sistemas de IA de alto riesgo (artículo 4, apartado 4 Resolución del Parlamento Europeo de 2020 sobre responsabilidad por IA). Este régimen se combina con la responsabilidad basada en la culpa, con presunción de negligencia para los sistemas de IA que no eran de alto riesgo. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial [2020/2014(INL)] (DO C 404 de 6.10.2021, p. 107).

⁷³ Al respecto, G. SPINDLER, “User liability and strict liability in the Internet of Things and for robots”, en S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p. 137.

Por otro lado, desde la perspectiva de las posibles víctimas y en relación con los derechos fundamentales, se ha señalado que la imposición de una responsabilidad verdaderamente objetiva genera consecuencias ambivalentes. Por un lado, esta responsabilidad estricta facilita la obtención de indemnizaciones, lo que refuerza la protección efectiva de los derechos fundamentales al vincular la responsabilidad con riesgos o violaciones de dichos derechos. Sin embargo, imponer una responsabilidad estricta sobre la IA sería una medida única a nivel global y, como se ha mencionado, podría ser vista como un obstáculo para la inversión, el desarrollo y la implementación de la IA en la UE. Esto podría tener repercusiones negativas para los derechos fundamentales, ya que una menor oferta de productos de IA en sectores clave podría privar a los consumidores y ciudadanos de innovaciones importantes, como vehículos autónomos que mejoren la seguridad vial, o servicios esenciales en la sanidad y la educación⁷⁴.

3. EL APOYO A LOS SISTEMAS DE IA INNOVADORES ANTES DE LA INTRODUCCIÓN EN EL MERCADO O PUESTA EN SERVICIO DESDE EL PERFIL DE LA RESPONSABILIDAD CIVIL

Una de las herramientas que la AIA ha previsto para apoyar la innovación son los espacios controlados de pruebas para la IA⁷⁵, donde se otorga a las pymes, incluidas las empresas emergentes unos beneficios para acceder a las mismas, orientaciones⁷⁶, formación específica y canales de comunicación adaptados también para los responsables del despliegue y, en su caso, para las autoridades públicas locales (art. 62.1 AIA). Se prevén algunas exenciones en las tasas para la evaluación de la conformidad (en virtud del artículo 43), incluso el acceso gratuito para las pymes (también empresas emergentes), si bien con la peculiaridad de que existan “costes excepcionales que las autoridades nacionales competentes puedan recuperar de una forma justa y proporcionada”, *ex* art. 58.2.d) AIA. Queda pendiente comprobar el éxito de la par-

⁷⁴ Como se anota en el *Complementary Impact Assessment*.

⁷⁵ Una exposición de las distintas medidas de apoyo a la innovación recogidas en el AIA, pueden consultarse en JIMÉNEZ SERRANÍA, V.: “Medidas de apoyo a la innovación y arquitectura de gobernanza”, cap. IV, El Reglamento Europeo de Inteligencia Artificial, dir. Barrio Andrés, M., Tirant lo Blanch, Valencia, pp. 111-138.

⁷⁶ Art. 58.3 AIA: Se ofrecerán a los proveedores potenciales que participen en los espacios controlados de pruebas para la IA, en particular a las pymes y las empresas emergentes, cuando proceda, servicios previos al despliegue, como orientaciones sobre la aplicación del presente Reglamento, otros servicios que aportan valor añadido, como ayuda con los documentos de normalización y la certificación, y acceso a las instalaciones de ensayo y experimentación, los centros europeos de innovación digital y los centros de excelencia.

ticipación al respecto que dependerá de los alicientes reales para invertir en este tipo de proyectos para las empresas emprendedoras, aunque se pretende que sirvan para impulsar la innovación y que los Estados miembros fomenten la participación en ellos (Considerandos 139 y 143)⁷⁷.

El art. 57.1 AIA determina que: “Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2026”. España ha sido pionera en materia de IA, aunque el art. 4.3 del Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, declara que ni los proveedores IA participantes, ni los usuarios participantes en el entorno controlado de pruebas “recibirán ningún tipo de contraprestación económica o en especie”⁷⁸.

La cuestión fundamental a los efectos analizados en este trabajo es averiguar hasta qué punto el “alivio regulatorio” que viene caracterizando a los partícipes en los “sandboxes”, repercute en el régimen de responsabilidad civil vigente durante la realización de las pruebas dentro y fuera de los espacios controlados para la IA. Descartamos que se pueda eximir de responsabilidad civil a los “proveedores o proveedores potenciales”⁷⁹, pese a que la doctrina lo ha llegado plantear, bajo este entorno de experimentación⁸⁰. De otro modo, sí se realiza una exención de multas siempre que se hubiera cumplido el plan

⁷⁷ Declara el Considerando (139) que “los espacios controlados de pruebas para la IA deben tener por objeto mejorar la seguridad jurídica de que gozan los innovadores y favorecer la vigilancia de las autoridades competentes y su entendimiento de las oportunidades, los riesgos emergentes y las consecuencias del uso de la IA, de facilitar el aprendizaje normativo de las autoridades y empresas, también con vistas a futuras adaptaciones del marco jurídico, de apoyar la cooperación y el intercambio de mejores prácticas con las autoridades que intervienen en el espacio controlado de pruebas y de acelerar el acceso a los mercados, también eliminando los obstáculos para las pequeñas y medianas empresas, incluidas las empresas emergentes. Los espacios controlados de pruebas para la IA deben estar ampliamente disponibles en toda la Unión y debe prestarse especial atención a que sean accesibles para las pymes, incluidas las empresas emergentes. La participación en el espacio controlado de pruebas para la IA debe centrarse en cuestiones que generen inseguridad jurídica y que, por lo tanto, dificulten que los proveedores y los proveedores potenciales innoven y experimenten con la IA en la Unión y contribuir a un aprendizaje normativo basado en datos contrastados”.

⁷⁸ Para una consulta del Sandbox IA español, véase: <https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Paginas/sandbox-IA.aspx>.

⁷⁹ Como ya justificamos en nuestro trabajo “La responsabilidad civil en los espacios controlados de pruebas (*regulatory sandboxes*)...”, cit.

⁸⁰ TRUBY, J. *et al.*: *Op. cit.*, p. 286. Por su parte, se critica a la AIA que los participantes en los entornos aislados de regulación de la IA seguirían siendo responsables de cualquier daño infligido a terceros debido a la experimentación en el entorno aislado, GONZÁLEZ TORRES, A.P./SAWHNEY, N.: “Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services”, *The Review of Socionetwork Strategies* (2023) 17, pp. 309-311.

específico y obrado de buena fe (art. 57.12 AIA), de dudosa justificación entendemos, y que por otro lado no se prevé cuando las pruebas se realicen en condiciones reales fuera de los espacios controlados para la IA⁸¹.

En virtud de la remisión que realiza el AIA “al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas” (art. 57.12), así como en el transcurso de las “pruebas en condiciones reales” (art. 60.9)⁸², no puede dejar de aplicarse el correspondiente régimen de responsabilidad civil ya vigente en cada ordenamiento jurídico para el sector de que se trate, en función de la actividad que procediera experimentar con IA⁸³. Así tuve ocasión de justificarlo con motivo de los sandboxes regulatorios en materia de movilidad inteligente, conforme se prevé en el PLMS.

En concreto, en beneficio no solo de los potenciales damnificados sino también del promotor (que pretende innovar con su proyecto), el art. 73.4 PLMS establece una adecuada responsabilidad solidaria expresa, en caso de imposibilidad de atribución proporcional por la intervención causal del promotor, al determinar que: “Cuando la responsabilidad no pueda imputarse al promotor ni al causante del daño se presumirá la existencia de una concurrencia de culpas entre el promotor, la autoridad o autoridades de supervisión involucradas y, en su caso, el causante del daño. En este caso, la responsabilidad será solidaria”⁸⁴. De otro modo, no parece muy incentivador de cara al promotor que piense en participar en estos espacios lo dispuesto en el Real

⁸¹ Véase sobre el reciente anuncio de imposición de sanciones por parte de AESIA, la noticia publicada en https://www.lavozdegalicia.es/noticia/coruna/2024/10/08/ignasi-belda-director-aesia-sanciones-comienzan-agosto/0003_202410H8C3991.htm.

⁸² Si bien el art. 60.9 AIA no se refiere expresamente “a terceros”, cabe deducir que ha sido la intención del legislador. Este precepto se ocupa de regular las pruebas de sistemas de IA de alto riesgo en condiciones reales *fuera de los espacios controlados de pruebas* para la IA.

⁸³ Sin embargo, en el caso español, la regulación que encontramos sectorial para distintos tipos de pruebas en entornos controlados, no es completa en lo que respecta a la regulación sobre responsabilidad civil y el correspondiente régimen de garantías. Y ello a pesar de lo dispuesto en el art. 16.3 y 4.f) de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes, que declara que: “Las pruebas se regirán por las normas sobre espacios controlados de pruebas que se dicten en cada sector y los protocolos que acuerden las autoridades supervisoras y los promotores de los proyectos, sin sujeción a la legislación específica del mercado de que se trate” y que: “La creación y desarrollo de los entornos controlados de pruebas se ajustarán a los siguientes principios de: “Protección de consumidores, de usuarios y de terceros que pudieran verse afectados por los riesgos potenciales de la innovación que se prueba”. De forma particular, nos ocupamos de analizar el sector de la movilidad previsto en el PLM, así como de algunos modelos de regulación en otros derechos en: “La responsabilidad civil en los espacios controlados de pruebas (*regulatory sandboxes*) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible”, cit., y “Análisis sobre las medidas de apoyo legal a la experimentación en tecnologías innovadoras”, cit.

⁸⁴ Respecto a otros aspectos no acertadamente regulados en la PLMS, como la remisión al régimen de garantías para establecer la responsabilidad civil, nos remitimos a “La responsabilidad

Decreto 568/2022, de 11 de julio, por el que se establece el marco general del mismo en el sector eléctrico es que se declara que “el promotor actuará a su riesgo y ventura y como único y exclusivo responsable de los daños y perjuicios derivados de sus incumplimientos e inobservancia de obligaciones previstas en el protocolo”, en la participación de los proyectos piloto en el banco de pruebas regulatorio previsto para el fomento de la investigación y la innovación en el sector eléctrico que regula el (art. 17).

Más adecuadamente, el art. 17 del Real Decreto 817/2023 declara la responsabilidad subjetiva conjunta entre los intervinientes en las pruebas, cuando dispone que “tanto el proveedor IA participante como, en su caso, el usuario participante será responsable de los daños sufridos por cualquier persona como consecuencia de la aplicación del sistema de inteligencia artificial en el contexto del entorno controlado de pruebas, siempre que dichos daños deriven de un incumplimiento o cuando medie culpa, negligencia o dolo por su parte”.

Al mismo tiempo, como ya se ha citado que contempla el PLMS, hay que traer a colación la posible responsabilidad patrimonial de la Administración, la cual cabría no solo en virtud de la participación activa en estas pruebas (como usuario o proveedor vgr. art. 3.7 y 3.8 Real Decreto 817/2023), sino también en su papel de supervisión y autorización de las autoridades competentes⁸⁵. Así se prevé expresamente en el PLMS (art. 73.3. *in fine*) lo que implica desde el punto de vista de la responsabilidad civil que la Administración tuviera que hacer frente al coste indemnizatorio por los daños irrogados a terceros en este ámbito previo a la introducción en el mercado o puesta en servicio. Huelga afirmar que las cláusulas de exención de responsabilidad a favor de las autoridades, pueden considerarse de dudosa legalidad, como tuvimos oportunidad de justificar (art. 69.2.g) PLMS o art. 12.1. *in fine* de la Ley 7/2020.

Además, vale la pena declarar que cuando una innovación de IA cumple con los requisitos regulatorios del “sandbox”, recibe un certificado de aprobación para su comercialización. Sin embargo, este sello no garantiza que el sistema esté exento de riesgos de responsabilidad en un futuro, pero a efectos de determinar

civil en los espacios controlados de pruebas (regulatory sandboxes) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible”, *op. cit.*

⁸⁵ Por su parte, el art. 58.4 AIA dispone que: “Cuando las autoridades nacionales competentes estudien autorizar la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA que se establecerá en virtud del presente artículo, acordarán específicamente las condiciones de dichas pruebas y, en particular, las garantías adecuadas con los participantes, con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con el fin de garantizar la coherencia de las prácticas en toda la Unión”. Sobre esta cuestión, véase TRUBY, J. *et al.*: *Op. cit.*, p. 286.

la diligencia a emplear por parte del proveedor o promotor, se podrá tener en cuenta si en el momento *ex ante* a su puesta en servicio, había mitigado el riesgo concreto de conocerlo, evidentemente. La AIA determina que “cualquier riesgo significativo detectado durante el proceso de desarrollo y prueba de estos sistemas de IA debe dar lugar a la adopción de medidas de reducción adecuadas y, en su defecto, a la suspensión del proceso de desarrollo y prueba” Considerando (139) AIA. Así como declara que “los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA deben proporcionar las garantías adecuadas y cooperar con las autoridades competentes, también siguiendo sus indicaciones y actuando con rapidez y de buena fe para mitigar adecuadamente cualquier riesgo considerable para la seguridad, la salud y los derechos fundamentales que se detecte y pueda surgir durante el desarrollo, las pruebas y la experimentación en dicho espacio” (Considerando 140).

Efectivamente, el “sandbox” de IA puede generar una falsa sensación de seguridad, ya que parece indicar que un sistema que ha pasado por esta evaluación no representa una amenaza para los derechos fundamentales o la seguridad. En realidad, un sistema de IA puede cumplir con la normativa, pero aun así generar riesgos imprevistos o evolucionar hacia una IA de alto riesgo a través de aplicaciones no previstas. El “sandbox” propuesto por la Unión Europea en la AIA, realmente, ofrece solo un tiempo limitado para evaluar el cumplimiento normativo de las innovaciones antes de su comercialización⁸⁶.

BIBLIOGRAFÍA

- ALEXANDER, C. et al.: “Safer not to know? Shaping liability law and policy to incentivize adoption of predictive AI technologies in the food system”, *Front. Artif. Intell.*, 2023.
- ALPA, G., “Quale modello normativo europeo per l’intelligenza artificiale?”, *Contratto e impresa*, 4/2021, 1003 a 1026.
- ATIENZA NAVARRO, M.L.: “La responsabilidad civil por daños causados por inteligencia artificial. estado de la cuestión”, *Derecho de Contratos, Responsabilidad Extracontractual e Inteligencia Artificial*, APPDC, coord.. N. Álvarez Lata, pp. 349-419.
- BATHAEE, Y.: “The Artificial Intelligence Black Box and the Failure of Intent and Causation.” *Harvard Journal of Law & Technology* 31 (2018): 889.
- BOEKEN, J.: “From compliance to security, responsibility beyond law”, *Computer Law & Security Review*, Volume 52, April 2024, 105926

⁸⁶ TRUBY, J. et al.: *Op. cit.*, p. 286.

- BUSTOS MORENO, Y. “The Implementation of U-space: Open Challenges from the Legal-Private Perspective”, Pastor Sempere, C. (Ed.). *Legal Framework for New Digital Assets, Identities and Data Space: Governance and Control of Data and Digital Economy in the European Single Market* [Subt. & Tit.]. Springer Cham. (Law, Governance and Technology Series; 16).
- “La responsabilidad civil en los espacios controlados de pruebas (regulatory sandboxes) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible”, *Cuadernos de Derecho Privado*, n. 2, 2022, pp. 8-49.
- “Análisis sobre las medidas de apoyo legal a la experimentación en tecnologías innovadoras”, *Revista Española de Derecho Aeronáutico y Espacial*, N.º 2 (Septiembre), 2022 (Ejemplar dedicado a: In memoriam excmo.sr.d. Rodolfo A. González-Lebrero), pp. 319-346.
- COMISIÓN EUROPEA: “Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme”, disponible en: <https://digital-strategy.ec.europa.eu/en/activities/testing-and-experimentation-facilities>
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on boosting startups and innovation in trustworthy artificial intelligence, COM/2024/28 final, pp. 9-10, <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52024DC0028>
- European Commission: Directorate-General for Communications Networks, Content and Technology, *European enterprise survey on the use of technologies based on artificial intelligence – Final report*, Publications Office, 2020, <https://data.europa.eu/doi/10.2759/759368>
- “Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety”, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, SWD(2021) 168 final, 2021
- DALMAU, J.: “La DGT ultima la normativa para la conducción autónoma”, *coches.net*, 6-2-2024, <https://www.coches.net/noticias/dgt-reglamento-conduccion-autonoma>
- DÍAZ ALABART, S.: *Robots y Responsabilidad Civil*, 2018, Reus.
- DÍAZ-RODRÍGUEZ, N. et al.: “Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulatio”, *Information Fusion Volume 99*, November 2023, 101896.
- EASA (2023) “Artificial Intelligence Roadmap 2.0 A human-centric approach to AI in aviation”, <https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20>.
- EVANGELIO LLORCA, R.: “Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad

- en las propuestas normativas de la UE”, *Derecho de Contratos, Responsabilidad Extracontractual e Inteligencia Artificial*, APPDC, coord.. N. Álvarez Lata, pp. 559-633.
- HELBERGER, N. /Diakopoulos, N.: “ChatGPT and the AI Act”, *Internet Policy Review* 12.1 (2023).
- GARCÍA MEXÍA, P. “Europa ante el reto de la inteligencia artificial”, *The Objective*, 3-8-2024, <https://theobjective.com/tecnologia/2024-08-03/europa-ante-el-reto-de-la-inteligencia-artificial/>.
- GONZÁLEZ TORRES, A.P./ SAWHNEY, N.: “Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services”, *The Review of Socionetwork Strategies* (2023) 17, pp. 297–318, <https://doi.org/10.1007/s12626-023-00146-y>
- HACKER, P.: “The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future”, *Computer Law & Security Review*, artículo 105871, Vol. 51, 2023, pp. 9-10.
- JIMÉNEZ SERRANÍA, V.: “Medidas de apoyo a la innovación y arquitectura de gobernanza”, cap. IV, *El Reglamento Europeo de Inteligencia Artificial*, dir. Barrio Andrés, M., Tirant lo Blanch, Valencia, pp. 111-138.
- JARUS: Methodology for Evaluation of Automation for UAS Operations, 2023.
- KARNER, E. et al.: “Comparative Law Study on Civil Liability for Artificial Intelligence”, estudio encargado por la Comisión Europea, Dirección General de Justicia y Consumidores al European Law Institute (ELI), 2021 (disponible en <https://data.europa.eu/doi/10.2838/66412>).
- KPMG (Trusted AI governance) ... Puede consultarse en https://media.lidn.com/dms/document/media/D4D1FAQGNtYPp0gfr1g/feedshare-document-pdf-analyzed/0/1728371213794?e=1729123200&v=beta&t=01_EQFBxCBnx8v-UgyLRCi2bb2TONVQk_oJQq5X3sQ p. 5.
- LAFUENTE SÁNCHEZ, R.: *Inteligencia artificial y vehiculos autónomos: Responsabilidad civil extracontractual internacional*, Aranzadi, 2024.
- MARCHISIO: “In support of ‘no-fault’ civil liability rules for artificial intelligence” (2021) 1 SN Social, <https://doi.org/10.1017/err.2021.52>
- MARÍN SALMERÓN, A.: *El defecto de diseño en los productos digitales*, Aranzadi, 2023.
- Algunas reflexiones sobre las propuestas de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos, *Contratación en el entorno digital* / coord. por Isabel González Pacanowska , María Carmen Plana Arnaldos, 2023, pp. 391-462.
- MUÑOZ VELA, J.M.: *La regulación de la inteligencia artificial. Reto y oportunidad desde una perspectiva global e internacional*, Aranzadi, 2024.
- OECD AI: “Investments in AI and data”, 2024, <https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-generative-ai-by-country>

- PARLAMENTO EUROPEO: *Complementary impact assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence*, Philip Hacker STUDY EPRS | Research Service Ex-Ante Impact Assessment Unit PE 762.861–September 2024.
- Resolución de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial [2020/2014(INL)] (DO C 404 de 6.10.2021,
- PASTOR, J. “La Unión Europea quiere dominar la revolución IA con regulación. Para los expertos es una mala idea”, *Xataka*, 13-12-2023, <https://www.xataka.com/robotica-e-ia/estallido-ia-se-ha-encontrado-viejo-enemigo-regulatorio-a-vuelta-esquina-efecto-bruselas>.
- RENDA, A. “Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe” Final report, European Commission, 2021.
- RUBÍ PUIG, A.: “Retos de la inteligencia artificial y adaptabilidad del derecho de daños”, *Retos jurídicos de la inteligencia artificial*, coord.. Cerrillo i Martínez, A./ Peguera Poch, M., pp. 57-71.
- SPINDLER, A.”User liability and strict liability in the Internet of Things and for robots”, en S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019.
- TRUBY, J. et al.: “A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications” *European Journal of Risk Regulation* (2022), 13, pp. 270-294. doi:10.1017/err.2021.52
- UNESCO C. Recommendation on the ethics of artificial intelligence (2020) Digital Library UNESDOC, URL en.unesco.org
- WANG, L., et. al.: “Human genome editing after the “CRISPR babies”: The double-pacing problem and collaborative governance”, *Journal of Biosafety and Biosecurity*, 5(1), 2023, pp. 8-13.

Responsabilidad civil e inteligencia artificial en el ámbito sanitario: posibles vías de reclamación¹

RAQUEL EVANGELIO LLORCA

*Profesora Titular de Derecho Civil
Universidad de Alicante*

Sumario: 1. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR SANITARIO. 2. RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR EL USO DE SISTEMAS DE INTELIGENCIA DE ARTIFICIAL EN EL ÁMBITO DE LA SANIDAD: CUESTIONES GENERALES. 3. DAÑOS CAUSADOS POR LA INTELIGENCIA ARTIFICIAL COMO PRODUCTO DEFECTUOSO. 3.1. Ámbito de aplicación del régimen de responsabilidad civil por daños causados por productos defectuosos. Los sistemas inteligentes como productos defectuosos. 3.1.1. El concepto de «producto» y la posible consideración del sistema inteligente como tal. 3.1.2. Un tipo específico de producto: el producto sanitario. 3.1.3. «Productos defectuosos», «componentes defectuosos» y sistemas inteligentes. 3.2. Sujetos responsables. 3.2.1. Determinación de los sujetos responsables. 3.2.2. Concurrencia de sujetos responsables. 3.3. Sujetos legitimados para ejercitar acciones por daños causados por productos defectuosos. 3.4. Fundamento de la responsabilidad y causas de exoneración. 4. RÉGIMEN DE RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR SERVICIOS SANITARIOS DEL ART. 148 TRLGDCU. 4.1. Ámbito de aplicación y fundamento de la responsabilidad. 4.2. Sujeto responsable. 4.3. Sujeto protegido. 5. RESPONSABILIDAD PATRIMONIAL DE LA ADMINISTRACIÓN SANITARIA. 6. RÉGIMEN DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL DEL CÓDIGO CIVIL. 7. CONSIDERACIONES FINALES SOBRE LA CONCURRENCIA DE RÉGIMENES APLICABLES. 8. BIBLIOGRAFÍA.

¹ Este trabajo se enmarca en el Proyecto I+D+i «La irrupción de la inteligencia artificial en el Derecho de daños y su adaptación a las nuevas tecnologías» (MICINN, 2021-2023), así como en el PROMETEO para grupos de investigación de excelencia «La nueva era de los algoritmos y la inteligencia artificial y su tutela jurídico-privada en el marco de la Unión Europea» (CIPROM/2022/40), financiado por la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital de la Generalitat Valenciana.

1 APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR SANITARIO

La inteligencia artificial (en adelante, IA)² es una pieza esencial en la denominada «salud digital» o e-Salud³, que puede entenderse como «el campo del conocimiento y la práctica relacionado con el desarrollo y la utilización de las tecnologías digitales para mejorar la salud»⁴ y que está siendo impulsada

² No existe una definición única y unánimemente aceptada de la IA. Ello se debe, en parte, a que se trata de un concepto en constante evolución, como consecuencia del incesante avance de la tecnología, y en otra parte, a que cubre numerosas aplicaciones heterogéneas que poco o nada tienen en común (sistemas de reconocimiento facial, *chatbots*, vehículos autónomos, sistemas de diagnóstico médico, robots de cocina o camareros, termostatos inteligentes, y un largo etcétera). Dado que el desarrollo de esta cuestión excede del propósito de este trabajo, me remito al análisis realizado en la bibliografía al respecto, así como a las definiciones recogidas en los diferentes textos y documentos emanados de las instituciones de la UE, y doy por válida la definición de «sistema de IA» recogida por el Reglamento del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), publicado en el DOUE núm. 1689 de 12.7.2024. De acuerdo con esta norma, un sistema de IA es un «sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales» (art. 3.1).

Cabe poner de relieve, por otro lado, que tanto en la denominación como en la propia concepción, los distintos instrumentos legislativos de la Unión Europea han experimentado cambios: por un lado, se ha pasado de la definición genérica de «inteligencia artificial» a la más específica de «sistemas de inteligencia artificial», y por otro, se ha añadido una nota relevante: la autonomía del sistema (Ver, por todos, NAVAS NAVARRO, S., *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022, pp. 10 y 12). En relación con ello, debo aclarar que en este trabajo utilizaré indistintamente los términos o expresiones «inteligencia artificial», «sistema inteligente» o «sistema de inteligencia artificial» para hacer referencia a la misma realidad. Asimismo, aludiré de forma indistinta a la IA o sistemas inteligentes o sistemas IA y a los robots, aunque técnicamente se entienda que no son lo mismo (Ver, sobre la distinción, ATIENZA NAVARRO, M.^a L., *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022, pp. 35 a 47; JORQUI AZOFRA, M., *Responsabilidad civil por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023, pp. 61-92).

³ Junto con otras tecnologías digitales avanzadas como el análisis masivo de datos (*big data*), las cadenas de bloques (*blockchain*), el Internet de las cosas (IoT) o las plataformas en línea. Ver, a este respecto, F. J. C., «Todas las claves de la transformación digital del sector salud», *El País*, 14 de diciembre de 2022, <https://elpais.com/sociedad/2022-12-14/todas-las-claves-de-la-transformacion-digital-del-sector-salud.html>

⁴ Se abordan diferentes aspectos del desarrollo de la IA en el ámbito sanitario en la *Estrategia España Digital 2026* y, dentro de ella, la *Estrategia Nacional de Inteligencia Artificial* (ENIA), <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf>; así como en la *Estrategia de Salud Digital. Sistema Nacional de Salud* de la Secretaría General de Salud Digital, Información e Innovación para el SNS, Ministerio de Sanidad, Gobierno de España (2021). https://www.sanidad.gob.es/areas/saludDigital/doc/Estrategia_de_Salud_Digital_del_SNS.pdf

tanto a nivel internacional por la Organización Mundial de la Salud (en adelante, OMS)⁵ como en el ámbito nacional⁶.

La aplicación de la IA en el ámbito de la salud abarca todos los sectores y crece de forma imparable.

Así, los sistemas inteligentes son muy útiles para la prevención de enfermedades o suicidios. En este sentido, un grupo de investigadores de la Universidad de Nottingham, en el Reino Unido, recopiló datos médicos rutinarios y sobre hábitos de vida de casi 400.000 pacientes y los utilizaron para entrenar un algoritmo capaz de predecir qué pacientes sufrirían infartos al cabo de 10 años con mejor precisión que los métodos convencionales⁷; y la Universidad de Valencia ha desarrollado un nuevo sistema de IA para detectar el cáncer de mama mediante el análisis de mamografías, que ha permitido alcanzar un 89% de diagnósticos precoces y reducir el número de falsos positivos⁸. Por otro lado, investigadores del Centro Médico de la Universidad de Vanderbilt, en Nashville, diseñaron un algoritmo capaz de predecir el riesgo de suicidio a partir de elementos como los datos de ingreso hospitalario, la edad, el sexo, la medicación y el historial diagnóstico⁹.

Los ensayos clínicos son otro prometedor campo para la IA, en la medida en que los algoritmos inteligentes pueden mejorar los criterios de elegibilidad ayudando a identificar a los voluntarios apropiados para los ensayos, lo cual es, a menudo, un factor limitante en las enfermedades raras¹⁰.

La IA también es muy eficaz en el campo del diagnóstico y el tratamiento con los «asistentes médicos inteligentes», como el robot *Watson* de IBM¹¹, que, mediante algoritmos que utilizan la minería masiva de datos, realizan un

⁵ OMS, *Estrategia mundial sobre salud digital 2020-2025*, 2021, <https://www.enfermeriacomunitaria.org/web/attachments/article/3224/Estrategia%20mundial%20sobre%20salud%20digital%202020-2025.pdf>

⁶ *Estrategia de Salud Digital...*, cit.

⁷ STRICKLAND, E., «AI Predicts Heart Attacks and Strokes More Accurately Than Standard Doctor's Method», *IEEE Spectrum*, 01 May 2017, <https://spectrum.ieee.org/ai-predicts-heart-attacks-more-accurately-than-standard-doctor-method>

⁸ https://www.uv.es/uvweb/uv-noticias/es/noticias/desarrollan-nuevo-sistema-ayuda-al-diagnostico-del-cancer-mama-basado-inteligencia-artificial-1285973304159/Novetat.html?id=1286030737530&plantilla=UV_Noticias/Page/TPGDetaillNews

⁹ GOLDHILL, O., «Artificial intelligence can now predict suicide with remarkable accuracy», *Quartz*, June 10, 2017, <https://qz.com/1001968/artificial-intelligence-can-now-predict-suicide-with-remarkable-accuracy>. Concretamente, el algoritmo fue capaz de predecir con una precisión del 92% los intentos de suicidio que se producirían a los pocos días, y con una precisión del 80-90% en los dos años siguientes.

¹⁰ ALKORTA, I., «Five crucial challenges for regulation of Medical artificial intelligence», *Revista Internacional de Estudios Vascos*, 67-2, p. 4.

¹¹ MOLLÁ, V., «IBM Watson al servicio de la medicina», 22 de enero de 2024, <https://www.victormolla.com/ibm-watson-medicina>

diagnóstico y protocolos de tratamiento muy precisos¹²; o el robot *Gower*, que lleva a cabo el suministro, mezcla y dispensación de medicamentos y fármacos con la finalidad de minimizar el error humano, calculando las dosis para quimioterapia¹³. Por otro lado, la rapidez con la que la IA puede procesar elevadas cantidades de datos es especialmente relevante a la hora de analizar diferentes pruebas médicas (resonancias, estudios genéticos...). Cabe referirse, igualmente, a las herramientas que permiten a los servicios de emergencias diagnosticar paradas cardíacas y otras dolencias mediante el análisis de la voz de la persona que llama, así como a los «nanobots», que son robots de tamaño nanométrico que pueden viajar por el interior del cuerpo humano para reparar tejidos o para combatir enfermedades, lo cual ofrece grandes posibilidades para el diagnóstico precoz y la dispensación de medicamentos¹⁴.

Otra interesante utilidad de los sistemas inteligentes es el seguimiento de los pacientes. En efecto, los dispositivos portátiles equipados con IA pueden monitorizar continuamente la salud del paciente, registrando parámetros como la presión arterial, la frecuencia cardíaca o los niveles de glucosa. Esto permite ajustes en tiempo real del tratamiento y envía alertas a los médicos si se detectan problemas, mejorando la gestión de enfermedades crónicas¹⁵. En esta línea, el Hospital Universitari Vall d'Hebron de Barcelona ha incorporado el asistente virtual del proyecto AZerca para mejorar el seguimiento de la enfermedad pulmonar obstructiva crónica (EPOC)¹⁶; y con carácter más

¹² En la misma línea, cabe mencionar a un grupo de ingenieros de la Escuela de Ingeniería Viterbi de la USC, en Estados Unidos, que ha desarrollado un algoritmo que podría minar los registros sanitarios electrónicos de las bases de datos para sugerir diagnósticos probables y pruebas diagnósticas útiles, acelerando y optimizando así los tratamientos (BALLON, M., «Healthier Healthcare», *USC Viterbi School of Engineering*, March 16, 2021, <https://viterbischool.usc.edu/news/2021/03/healthier-healthcare/>).

¹³ RAMÓN FERNÁNDEZ, F., «Inteligencia artificial en la relación médico-paciente: Algunas cuestiones y propuestas de mejora», *Revista Chilena de Derecho y Tecnología*, vol. 10, núm. 1, 2021, p. 334.

¹⁴ GIL MEMBRADO, C., «Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el Derecho», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, p. 358.

¹⁵ REDACCIÓN APD, «Efectos de la inteligencia artificial en la medicina y sus aplicaciones más novedosas», 16 agosto 2024, <https://www.apd.es/aplicaciones-inteligencia-artificial-en-medicina/>

¹⁶ Según explica MIRIAM BARRECHEGUREN, adjunta del servicio de Neumología del Vall d'Hebron y responsable del proyecto AZerca, el objetivo principal es realizar un seguimiento personalizado de los pacientes que sufren esta enfermedad y reducir la carga asistencial. «Lo vamos a utilizar -afirma- en un estudio que incluirá a pacientes con EPOC agudizadores, reclutando desde consultas, tanto a aquellos que presentan agudizaciones frecuentes como a aquellos que ingresan por una agudización grave de la EPOC. Para ello, este asistente llamará a los pacientes con una periodicidad semanal para evaluar cuál es su situación clínica mediante una serie de preguntas y cuestionarios de síntomas» (SÁNCHEZ CAJA, A., «La aplicación de la IA en los hospitales puede reducir hasta un 50% el coste de la atención al paciente», *EDS Revista Española de Economía de la Salud*, 16 febrero 2024, <https://economiadelasalud.com/topics/difusion/la-aplicacion-de-la-ia-en-los-hospitales-puede-reducir-hasta-un-50-el-coste-de-la-atencion-al-paciente/>).

general, el *chatbot Florence* puede actuar como enfermera virtual para recordar a los usuarios que tomen sus medicamentos, hacer un seguimiento de su salud o localizar la farmacia o el médico más cercanos¹⁷. En este punto es preciso mencionar, asimismo, los medicamentos digitales, cuyo propósito inicial es mitigar el grave problema de la mala adherencia a los tratamientos terapéuticos por parte de los pacientes; estos dispositivos permiten rastrear la ingesta del medicamento con una precisión nunca vista antes, así como otro tipo de información médica del paciente (frecuencia cardíaca, actividad física, calidad del sueño), y remitir la información a un parche que el paciente lleva adherido a su cuerpo, y de ahí a otro dispositivo (el teléfono inteligente del paciente), desde el cual es enviada, al mismo tiempo, al portal sanitario de su médico¹⁸.

No podemos olvidar tampoco el campo de la cirugía, en la que ciertos robots quirúrgicos, como STAR, llevan a cabo intervenciones quirúrgicas sin intervención humana con un alto nivel de precisión, seguridad y efectividad¹⁹.

De igual forma, existen robots muy eficientes en procesos de rehabilitación, como el *Lokomat*, diseñado para la rehabilitación funcional de la marcha en personas que sufren secuelas producidas por un daño neurológico tanto a nivel cerebral como en la médula espinal²⁰; así como prótesis inteligentes, que aprenden de la persona que la lleva, adaptándose mucho mejor a sus necesidades y movimientos²¹.

¹⁷ EBERS, M., «¿Terapia sin terapeutas?: la interacción persona-robot en el marco del Reglamento sobre productos sanitarios de la UE y la Ley de Inteligencia Artificial», en *Servicios privados de telemedicina y salud digital: retos e implicaciones jurídicas*, dir. por R. Luquin Bergareche, Tirant lo Blanch, Valencia, 2023, p. 78.

¹⁸ MORLA GONZÁLEZ, M., «Problemas jurídicos que plantean las terapias digitales para el rastreo del comportamiento del paciente», en *El Derecho y la justicia ante la inteligencia artificial y otras tecnologías disruptivas*, dir. por M. Castilla Barea y M.^a D. Cervilla Garzón, Aranzadi, Madrid, 2024, p. 613.

¹⁹ Ver FRUTOS, Á., «Un robot realiza sin ayuda humana y con gran éxito la primera cirugía en tejido blando», *La Vanguardia*, 1 febrero 2022, <https://www.lavanguardia.com/tecnologia/20220201/8023051/robot-cirugia-sin-humanos-nbs.html>. Es preciso mencionar, asimismo, el famoso robot quirúrgico *Da Vinci* (<https://www.abexsl.es/es/sistema-robotico-da-vinci/que-es>), si bien en este caso es el cirujano quien en realidad controla este instrumento (compuesto por una cámara-brazo y un brazo mecánico, que tiene una serie de instrumentos en su extremo) puesto que dispone de la visión de una pantalla de alta definición, ampliada y a tres dimensiones. Por ello se dice que este tipo de instrumentos no pueden calificarse como sistemas de IA, dado que, «a pesar de su naturaleza disruptiva e innovadora, no es diferente, en el fondo, a herramientas menos adelantadas tecnológicamente» (ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 367).

²⁰ <https://neuronrehab.es/blog/rehabilitacion-funcional-lokomat/>

²¹ REDACCIÓN APD, «Efectos de...», cit., donde se apunta que se trata de apéndices mecánicos que no solo sustituyen a un miembro del cuerpo, sino que memorizan los patrones de movimiento de la persona y pueden ser controlados mediante una aplicación.

De la misma manera, la IA puede prestar un gran servicio en la gestión sanitaria. Pensemos, por ejemplo, en su uso para el sistema de triaje (e-triage), avalado por estudios científicos²² y ya una realidad en los servicios de urgencias²³; en el desarrollo de modelos para optimizar la planificación en los servicios de hospitales; en las UCI, donde robots, como *Assum*, desinfectan espacios mediante luz ultravioleta o se desplazan para atender a pacientes que requieren un seguimiento continuo y a la vez un control remoto del médico humano que puede, de forma eficiente, realizar simultáneamente el seguimiento de varios pacientes²⁴; o en la gestión del inventario de suministros médicos, asegurando que siempre haya disponibilidad de medicamentos y equipos críticos.

En este breve repaso al uso de la IA en el ámbito sanitario es preciso hacer referencia, asimismo, a la salud móvil o m-Salud (*m-Health*), que representa un segmento de la e-Salud y que comprende, por un lado, «la práctica de la medicina y la prestación de servicios sanitarios mediante los dispositivos móviles, como teléfonos móviles, dispositivos de seguimiento de pacientes, asistentes digitales personales (PDA, en sus siglas en inglés) y otros dispositivos inalámbricos»; al tiempo que incluye «aplicaciones tales como las de modo de vida y bienestar que pueden conectarse a dispositivos médicos o sensores (por ejemplo, brazaletes o relojes)», así como «dispositivos de orientación personal, información sanitaria y recordatorios de medicación mediante el envío de mensajes de texto y la telemedicina inalámbrica»²⁵.

El último paso se ha dado en China, donde acaba de inaugurarse el *Agent Hospital*, que es el primer hospital del mundo que funciona completamente mediante IA. Se trata, en efecto, de un entorno simulado donde los pacientes pueden acceder a atención médica a través de una plataforma digital, y cuyos 14 médicos y 4 enfermeras, todos ellos generados mediante tecnología de últi-

²² INFOSALUS, «La IA demuestra su utilidad en el triaje de pacientes de Urgencias», 10 mayo 2024, <https://www.infosalus.com/asistencia/noticia-ia-demuestra-utilidad-triaje-pacientes-urgencias-20240510071450.html>

²³ El Servicio de Urgencias del Hospital General Mancha Centro ha recibido un galardón al mejor proyecto de inteligencia artificial en la ceremonia de entrega de los “15 Premios Comunicaciones Hoy”, por el desarrollo de una herramienta basada en inteligencia artificial que mejora el sistema de triaje tradicional (REDACCIÓN CMM, «Así ayuda la Inteligencia Artificial al triaje de las urgencias», *CMM Noticias*, 27 noviembre 2023, <https://www.cmmmedia.es/noticias/castilla-la-mancha/asi-ayuda-inteligencia-artificial-triaje-urgencias.html>).

²⁴ LUQUIN BERGARECHE, R., «Responsabilidad contractual por el uso de la IA en la prestación de servicios de telemedicina y aplicaciones de salud digital», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, p. 300.

²⁵ COMISIÓN EUROPEA, *Libro Verde sobre sanidad móvil*, Bruselas, 10.4.2014 COM(2014) 219 final, p. 3, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52014DC0219>

ma generación, están capacitados para atender a unos 3.000 pacientes diarios. Las ventajas de este tipo de hospitales son evidentes: los pacientes pueden interactuar con los médicos de IA desde cualquier lugar, sin desplazarse, lo que es fundamental para personas en áreas remotas o con dificultades de movilidad; además, el hospital no está sujeto a las restricciones de tiempo o descanso que enfrentan los médicos humanos, esto porque la IA puede operar de manera continua, proporcionando atención las 24 horas del día. De este modo, representa una alternativa muy tentadora ante los problemas de saturación y falta de recursos suficientes para atender a toda la población de manera eficiente que tienen los hospitales tradicionales en muchos países, puesto que es capaz de reducir los tiempos de espera y aumentar la capacidad de atención sin necesidad de construir infraestructura adicional o aumentar el número de profesionales de la salud²⁶.

2. RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR EL USO DE SISTEMAS DE INTELIGENCIA DE ARTIFICIAL EN EL ÁMBITO DE LA SANIDAD: CUESTIONES GENERALES

Junto con sus múltiples ventajas, son también variados los peligros e inquietudes que el uso de la IA plantea en el ámbito sanitario²⁷. Entre ellos, cabe mencionar el riesgo de deshumanización de la relación médico-paciente y las dudas sobre la capacidad de los sistemas de IA para tomar decisiones éticas y humanizadas. En efecto, la toma de decisiones médicas frecuentemente implica consideraciones emocionales, éticas y sociales que son difíciles de programar en una máquina²⁸. A este respecto, debe recordarse la advertencia de las instancias europeas de que la salud digital no debe conducir a la deshumanización de los cuidados y la reducción de la relación entre médico y paciente, sino que debe orientarse a proporcionar al profesional ayuda para el diagnóstico y el tratamiento más efectivo de los pacientes²⁹. De igual forma,

²⁶ ESCOBAR RUIZ, D., «Crean el primer hospital operado por robots e Inteligencia Artificial: qué pasó con los médicos», *Infobae*, 8 septiembre 2024, <https://www.infobae.com/tecnologia/2024/09/08/crean-el-primer-hospital-operado-por-robots-e-inteligencia-artificial-que-paso-con-los-medicos/>

²⁷ NAVARRO MENDIZÁBAL, I., «¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos», *Revista Iberoamericana de Bioética*, núm. 25, p. 4, apunta que estamos en un momento de «reflexión adversativa»: «Somos conscientes de las enormes ventajas de la IA, *pero*... y toda reflexión y consideración que se realiza siempre tiene ese *pero*... Da igual la faceta humana de la que tratemos, siempre vemos la ventaja de la IA y su *pero*».

²⁸ ESCOBAR RUIZ, D., «Crean el primer...», cit.

²⁹ Así lo recordó la Comisión de medio ambiente, salud pública y seguridad alimentaria (16.9.2020) en su Opinión para la Comisión de Asuntos Jurídicos en relación con la Propuesta de Resolución del Parlamento Europeo (convertida en Resolución el 20 octubre 2020) con recomenda-

el uso de los «nanobots», por ejemplo, genera ciertos reparos por el hecho de la introducción en el cuerpo de mecanismos que pueden controlar los procesos celulares o incluso la conducta humana si se instalan en el cerebro y en el sistema nervioso³⁰.

Además de lo anterior, el uso de sistemas inteligentes en el sector sanitario puede provocar, y de hecho provoca, diferentes daños. En efecto, se producen equivocaciones de diagnóstico o tratamiento, errores en la dispensación de medicamentos, fallos de los brazos robóticos en cirugía, recogida ilegal de datos personales, discriminación en el triaje de pacientes o el acceso a los tratamientos o aun trasplante de órganos, errores en el funcionamiento de las listas de espera, etc., que causan perjuicios de diversa naturaleza a los pacientes.

Lógicamente, la persona que haya sufrido algún daño como consecuencia de la utilización de herramientas de IA en el ámbito sanitario querrá ser indemnizada. Es más, pese a que la IA no ha incrementado -ni parece que vaya a hacerlo- los daños en muchos sectores de actividad donde se ha introducido, e incluso en algunos ámbitos los reduce considerablemente en relación con la actuación exclusivamente humana³¹, y aunque estos daños no revisten unas características propias y diferentes a los daños causados de ordinario por otras tecnologías o por una actividad o comportamiento humanos³², existe una especial preocupación por asegurar la indemnización por los daños que causen las tecnologías basadas en IA. Entre las razones para ello probablemente se encuentra el hecho de que existe un elevado grado de desconfianza respecto de las tecnologías basadas en la inteligencia artificial, debido a que en ocasio-

ciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)), disponible en https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_ES.html#_section11. La Comisión añadía a lo anterior que los pacientes deben saber cuándo y cómo interactúan con un profesional humano y cuándo no, deben tener la libertad de decidir a este respecto y se les debe ofrecer una alternativa de nivel equivalente.

³⁰ GIL MEMBRADO, C., «Una nueva era...», cit., p. 358.

³¹ RACHUM-TWAIG, O., «Whose robot is it anyway?: Liability for artificial-intelligence-based robots», 2020 *Univ. Ill. L.Rev.* 4, p. 1158; RUBÍ PUIG, A., «Retos de la inteligencia artificial y adaptabilidad del Derecho de Daños», en Cerrillo i Martínez, A./Peguera Poch, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2020, p. 60; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 25.

Por lo que se refiere al ámbito médico, como señala FERRETTI, F., «Intelligenza Artificiale e responsabilità civile nel settore sanitario», *Actualidad Jurídica Iberoamericana*, núm. 18, febrero 2023, p. 1858, el uso de la IA ha mejorado el nivel de eficiencia en la prestación sanitaria, reduciendo los riesgos de errores del personal humano y aumentando a la vez el nivel de seguridad de los cuidados. Además, esta tecnología reduce el grado de invasión de las intervenciones y las dolencias físicas y disminuye el tiempo de rehabilitación del paciente.

³² Ver, en relación con este punto, RUBÍ PUIG, A., «Inteligencia artificial y daños indemnizables», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 621-688.

nes escapan del control humano directo³³; que la sociedad moderna es muy sensible, en general, a la producción de daños y «no parece estar dispuesta a asumir, como si se tratara de una fatalidad inevitable, los daños que puedan causar las nuevas tecnologías, en general, y los sistemas de IA, en particular»³⁴; y que los daños causados por la IA son especialmente relevantes, en la medida en que pueden afectar a derechos de la personalidad, como la igualdad, la intimidad, la privacidad, la protección de datos y la libertad de expresión, por citar algunos de ellos³⁵. Pero el principal motivo, a mi juicio, de esta preocupación por garantizar la indemnización de los daños causados por sistemas inteligentes es la dificultad de identificar la causa concreta del daño e imputar jurídicamente este cuando interviene una IA compleja o cuando, como es habitual, son numerosos los sujetos que podrían tener responsabilidad. En el ámbito de la salud, que es el que nos interesa, pensemos que los daños pueden deberse a causas tan diversas como defectos de diseño del programa informático, defectos de diseño o fabricación del producto, falta de actualizaciones adecuadas, sesgos en el entrenamiento de los sistemas inteligentes, maniobras defectuosas del personal sanitario o incluso una combinación de algunos de estos factores³⁶.

Además, las características de los SIA pueden hacer muy difícil identificar la causa del daño. Tales características son las siguientes: complejidad, opacidad, apertura, autonomía, imprevisibilidad, dependencia de los datos y vulnerabilidad³⁷. Veámoslas brevemente.

³³ ELIZALDE SALAZAR, I., *Vehículos autónomos. Responsabilidad civil y seguro*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2022, pp. 45-46, quien añade que, además, aceptamos mejor el error humano que el de una máquina, lo cual, como apunta ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 25, y «La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, p. 343, ha originado socialmente una cierta «robophobia».

³⁴ MARTÍN CASALS, M., «Desarrollo tecnológico y responsabilidad extracontractual: a propósito de los sistemas de Inteligencia Artificial (IA)», en *La cultura jurídica en la era digital*, coord. por Pérez Collados, J. M., Aranzadi, Cizur Menor (Navarra), 2022, p. 137.

³⁵ ATIENZA NAVARRO, M.^a L., «La responsabilidad civil...», cit., p. 345.

³⁶ DE LORENZO APARICI, O., «¿Pueden todas las aplicaciones de salud considerarse productos sanitarios?», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, p. 100, recuerda el caso de Therac-25, un acelerador lineal de radioterapia que ocasionó el fallecimiento de cuatro pacientes como consecuencia de una sobredosis de radiación secundaria debida a un mal funcionamiento del *software* y unas prácticas de desarrollo inadecuadas.

³⁷ A ellas se hace referencia en el Informe *Liability for artificial intelligence and other emerging digital technologies* (disponible en https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf) elaborado por el Grupo de Expertos en responsabilidad civil y nuevas tecnologías (*Expert Group on Liability and New Technologies - New Technologies Formation*) por encargo de la CE, la cual, en su Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Inteligencia artifi-

- a) La complejidad procede de la combinación del *hardware* y el *software* implicados en esta nueva tecnología³⁸ y se define como el alto grado de sofisticación técnica que necesitan las múltiples partes del *hardware* actual para su interacción, combinada con el creciente porcentaje de componentes digitales, incluyendo la inteligencia artificial³⁹.
- b) La opacidad (denominada también «efecto de caja negra» o «*black box*»), consiste en la dificultad para comprender y explicar cómo han tomado sus decisiones los sistemas de inteligencia artificial⁴⁰. En relación con ello, ciertos autores distinguen los conceptos de interpretabilidad y explicabilidad de la IA. La primera se concibe como una aproximación a la explicación *ex ante*, con anterioridad a la toma de decisión por parte del sistema inteligente; mientras que la explicabilidad conlleva un examen *ex post*, puesto que implica centrarse en el

cial para Europa», Bruselas, 25.4.2018, COM(2018) 237 final, pp. 11 y 17, <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2018%3A237%3AFIN>, anunció la creación del aludido Grupo de Expertos y le encargó la elaboración de un informe en el que se evaluarán los retos que plantean algunas características de la inteligencia artificial respecto de la responsabilidad civil (p. 19). Ya antes del citado Informe, los rasgos apuntados de la IA fueron puestos de manifiesto por la CE en su previo documento de trabajo «Liability for emerging digital technologies» accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe [COM(2018) 237 final], Brussels, 25.4.2018 SWD(2018) 137 final, <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137> (sólo disponible en inglés), pp. 10 y 23, y recogidos después en su Informe al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo «Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica», Bruselas, 19.2.2020 COM(2020) 64 final, <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020DC0064>, p. 2., que acompañaba al *Libro Blanco sobre la inteligencia artificial -un enfoque europeo orientado a la excelencia y la confianza* de 19 de febrero de 2020, COM(2020) 65 final, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> (en adelante, Libro Blanco sobre IA).

También en la doctrina es ya lugar común hacer referencia a las características señaladas. Ver, entre otros, ATAZ LÓPEZ, J., «Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial», *Working paper 4/2020*, Working papers Jean Monnet Chair - European Private Law, Universitat de Barcelona, pp. 27-29; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., pp. 56-66; RODRÍGUEZ DE LAS HERAS BALLELL, T., «La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial», *La Ley Mercantil*, núm. 103, Sección Derecho Digital, junio 2023, pp. 4-6; HERBOSA MARTÍNEZ, I., «Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos», *InDret*, 3.2024, pp. 63-68.

³⁸ ATAZ LÓPEZ, J., «Daños causados...», cit., 27.

³⁹ GRUPO DE EXPERTOS, Informe NTF 2019, pp. 32-33.

⁴⁰ MARTÍN CASALS, M., «Desarrollo tecnológico...», cit., p. 116, y «La regulación de la responsabilidad extracontractual por daños causados por sistemas de Inteligencia Artificial (IA)», *RC-Revista de Responsabilidad Civil y Seguro*, año 60, núm. 1, enero 2023, p. 6.

conocimiento que ha dado lugar a la toma de una decisión en una situación concreta⁴¹.

Por lo que se refiere al ámbito sanitario, el Reglamento General de Protección de Datos de 2016⁴² (en adelante, RGPD) contempla la obligación de proporcionar información a los pacientes sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, «y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado» [arts. 13.2 f) y 14.2 g) RGPD]. El alcance de esta previsión no está claro; en opinión de GIL MEMBRADO, el deber de información quedará cumplido cuanto el médico responsable informe a un paciente, con carácter general, sobre los pormenores del SIA que se va a usar para analizar una imagen, sin que se exija que le informe sobre la lógica decisional específica que ha arrojado un determinado diagnóstico al someter su prueba de imagen a los dictados de la IA. En definitiva, según la citada autora, el derecho a la información previsto por el RGPD se materializa en un derecho a la interpretabilidad, pero no a la explicabilidad, en los términos expuestos⁴³.

La Agencia Española de Protección de Datos (AEPD), en cambio, sostiene que para cumplir con la obligación de proporcionar información «significativa», que según la RAE denota «[q]ue da a entender o conocer con precisión algo», debe facilitarse información que permita entender el comportamiento del tratamiento⁴⁴.

El art. 22 RGPD, por su parte, dedicado específicamente a las decisiones automatizadas, establece que, en los casos a que se refiere

⁴¹ GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Reus, Madrid, 2023, p. 142, que cita, a su vez, a MAGDALENA LAYOS, L., «Por qué debería confiar en ti (máquina)», en *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, Madrid, 2021, dir. por Lledó Yagüe, F., Benítez Ortúzar, I. y Monje Balmaseda, Ó., Dykinson, Madrid, 2021, p. 636. Con un punto de vista diferente, BUSTINCE SOLA, H., Doctor en Matemáticas y Catedrático de Ciencias de la Computación, en su ponencia «La IA explicable», *I Congreso Internacional Digitalización e Inteligencia Artificial en la contratación y prestación de servicios médicos*, UPNA, Pamplona, 4 de octubre de 2024, afirma que la explicabilidad se refiere a que el SIA sepa decir por qué ha llegado a un resultado, mientras que la interpretabilidad significa que el usuario sea capaz de entender, una vez que los pueda conocer, qué pasos han llevado al modelo a la respuesta dada.

⁴² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

⁴³ GIL MEMBRADO, C., *Riesgos del uso...*, cit., pp. 141-142.

⁴⁴ AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, febrero de 2020, disponible en <https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf>.

el apartado 2, letras a) y c) -esto es, cuando una decisión automatizada es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento o se basa en el consentimiento explícito de aquel-, el responsable del tratamiento «adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión». Algún autor estima que este precepto atribuye a los pacientes el derecho a entender cómo un sistema inteligente ha adoptado determinada decisión sobre una cuestión de salud (p. ej., para decidir sobre la prioridad de un tratamiento médico)⁴⁵; en realidad, tal derecho no se recoge de forma explícita, aunque podría entenderse incluido con base en el cdo. 71 del Reglamento, que expresamente declara que el tratamiento de datos «debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión»⁴⁶.

Cabe preguntarse si el derecho a la información sobre la lógica decisional del algoritmo puede derivar de la Ley 41/2002 Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. El art. 4 de esta norma atribuye al paciente un derecho a la información asistencial, que incluye el derecho a conocer, con motivo de cualquier actuación sobre su salud, toda la información disponible, salvo las excepciones previstas por la ley. Es razonable entender que entre la información que el médico debe proporcionar se encuentra la relativa al funcionamiento del sistema inteligente que eventualmente se utilice. Ahora bien, este deber se ha de exigir teniendo en cuenta las posibilidades del facultativo, que en muchos casos no conocerá la lógica decisional del algoritmo⁴⁷.

- c) La apertura significa que los sistemas inteligentes no se ponen en circulación como sistemas completos, sino que, por su propia naturaleza, necesitan mantenerse abiertos, ya que dependen de *inputs* pos-

⁴⁵ ALKORTA, I., «Five crucial challenges...», cit., pp. 8-9.

⁴⁶ En opinión de GIL MEMBRADO, C., *Riesgos del uso...*, cit., p. 139, el hecho de que el RGDP no apunte la obligación de información específica en el articulado y solamente se recoja en un considerando, hace dudar de que se llegue a recoger como una garantía.

⁴⁷ En el mismo sentido, GIL MEMBRADO, C., *Riesgos del uso...*, cit., p. 45.

teriores, especialmente de actualizaciones y mejoras, o de interconexiones con otros sistemas de datos para funcionar correctamente⁴⁸.

- d) La autonomía hace referencia a la capacidad de los sistemas inteligentes para realizar tareas con poco control o supervisión humana, o incluso sin ninguno; es decir, para tomar sus propias decisiones, al menos hasta un cierto punto, ante posibles alternativas de actuación, sin que la elección de una opción específica por parte del sistema de inteligencia artificial esté determinada por los datos proporcionados por su diseñador⁴⁹.

Ahora bien, hoy por hoy en el ámbito de la UE no se permite la utilización de sistemas inteligentes sin que haya control humano en mayor o menor medida. En efecto, el art. 14 RIA impone el deber de diseñar y desarrollar los sistemas inteligentes de modo que se permita una vigilancia efectiva por personas físicas durante el período de su utilización, con el objetivo de «prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo»⁵⁰ conforme a su

⁴⁸ GRUPO DE EXPERTOS, Informe NTF 2019, p. 33; KOCH, B./BORGHETTI, J. B./MACHNIKOWSKI, P./PICONNAZ, P./RODRÍGUEZ DE LAS HERAS BALLELL, T./TWIGGFLESNER, C./WENDEHORST, C., *Response of the European Law Institute (ELI) to the European Commission's Public Consultation on Civil Liability - Adapting Liability Rules to the Digital Age and Artificial Intelligence*, 2022, p. 26, disponible en https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf. En la misma línea, MARTÍN CASALS, M., «Desarrollo tecnológico...», cit., p. 117; y ATIENZA NAVARRO, M. L., «¿Una nueva responsabilidad por productos defectuosos?», *Indret*, 2.2023, p. 12.

⁴⁹ MARTÍN CASALS, M., «Desarrollo tecnológico...», cit., p. 116, que remite a RUSSELL, S. J./NORVIG, P., *Artificial Intelligence: A Modern Approach*, 4th ed., Global Edition (Harlow: Pearson, 2022), p. 60, y CHESTERMAN, S., *We, The Robots? Regulating Artificial Intelligence and the Limits of the Law* (Cambridge: Cambridge University Press, 2021), pp. 31 y ss.

⁵⁰ El RIA adopta un enfoque basado en el riesgo, a partir del cual clasifica los sistemas de IA en cuatro categorías de riesgo distintas, adaptando el tipo y contenido de sus normas a la intensidad y alcance de dichos riesgos que presentan los sistemas de IA sobre los que se aplica: riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo. Entre los sistemas de alto riesgo se incluyen los productos regulados, que son aquellos destinados a utilizarse como componente de seguridad en determinados productos regulados o el mismo sistema de IA sea un producto regulado. Se encuentran identificados en el Anexo I del Reglamento y entre ellos se encuentran, entre otros, los productos sanitarios (además de, p. ej., juguetes, automóviles, aviones, embarcaciones). De igual forma, el Anexo III del Reglamento identifica como de especial relevancia o sensibles algunos usos de la IA en ámbitos como la biometría, servicios financieros, centros educativos o laborales, acceso a servicios esenciales (entre los que se incluyen servicios sanitarios, de emergencias o financieros), policía, migración y asilo, administración de justicia o procesos electorales; salvo que no planteen riesgos de considerable perjuicio a los derechos y libertades fundamentales de las personas físicas (por ejemplo, si su finalidad es realizar una tarea procedimental limitada, optimizar el resultado de una actividad previamente realizar o detectar pautas o desviaciones de las pautas de toma de decisiones sin el objeto de sustituir o influir en la evaluación humana, y en tanto en cuanto no impliquen un perfilado).

finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos establecidos en la presente sección»⁵¹.

Así, en el ámbito sanitario, todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar (salvo ciertas excepciones, recogidas en el art. 22 RGPD). Los EEMM, por tanto, deben implantar mecanismos apropiados para garantizar el derecho del afectado a obtener intervención humana⁵².

- e) La (im)previsibilidad en la actuación de los sistemas inteligentes es una consecuencia inevitable de su autonomía y será mayor cuantos más datos externos sean capaces de procesar y más sofisticados sean⁵³, así como cuanto menos necesiten de la intervención humana⁵⁴.
- f) La dependencia de los datos procede de que los sistemas inteligentes precisan de información externa que no estaba pre-instalada, sino que es generada por sensores incorporados o comunicada desde el exterior, ya sea por fuentes de datos regulares o por proveedores *ad hoc*.
- g) La vulnerabilidad, por fin, es consecuencia del diseño abierto de los sistemas inteligentes y de su interconectividad. En efecto, la introducción de mejoras y actualizaciones, así como la recepción de datos externos, pueden incidir en el funcionamiento del sistema; además, hacen que los sistemas inteligentes sean muy vulnerables a ciberataques, los cuales pueden provocar, asimismo, un mal funcionamiento⁵⁵; si bien algunos de estos ataques pueden ser fácilmente detectados con sistemas de alertas⁵⁶.

⁵¹ A este respecto, el precepto dispone que las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo.

En opinión de MUÑOZ VELA, J. M., *Retos, riesgos, responsabilidad y regulación de la inteligencia artificial*, Thomson Reuters Aranzadi, 2022, p. 207, y GIL MEMBRADO, C., *Riesgos del uso...*, cit., p. 167, tanto ahora como en el futuro, los SIA siempre deberían estar controlados y supervisados por humanos.

⁵² ALKORTA, I., «Five crucial challenges...», cit., pp. 8-9.

⁵³ Así lo pone de relieve el Informe NTF 2019, p. 33.

⁵⁴ MASCITTI, M., «La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos», *Revista de Derecho Privado*, núm. 42, 2022, pp. 224 y 233.

⁵⁵ GRUPO DE EXPERTOS, Informe NTF 2019, p. 33; KOCH, B./BORGHETTI, J. B./MACHNIKOWSKI, P./PICONNAZ, P./RODRÍGUEZ DE LAS HERAS BALLELL, T./TWIGG-FLESNER, C./WENDEHORST, C., *Response of the...*, cit., p. 26.

⁵⁶ MA X., NIU Y., GU L., ET AL., «Understanding adversarial attacks on deep learning based medical image analysis systems», *Pattern Recognit*, 2021, 110:107332, <https://doi.org/10.1016/j.patcog.2020.107332>.

Todas estas características dificultan, como decía, la identificación de la causa del daño, hasta el punto de convertir la prueba del nexo de causalidad -que, como es sabido, de acuerdo con las reglas generales del procedimiento corresponde al demandante- en imposible o prohibitivamente cara⁵⁷. Por ello, y dado que la clave del éxito de cualquier pleito reside en la prueba de los hechos que se alegan, no debe extrañar que en las iniciativas de la UE relacionadas con la responsabilidad civil por uso de la inteligencia artificial [a saber, la Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos presentada por la Comisión Europea (en adelante, CE) el 28 de septiembre de 2022 y aprobada en primera lectura por el Parlamento Europeo (en adelante, PE) el 12 de marzo de 2024 (en adelante, PDRDPD)⁵⁸, y la Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil e inteligencia artificial (en adelante, PDRIA)⁵⁹, presentada en la misma fecha y que, a diferencia de la anterior, tiene un futuro más incierto⁶⁰]⁶¹, los problemas relacionados con la causalidad y su prueba ocupen un lugar preeminente.

⁵⁷ DE BRUYNE, J., VAN GOOL, E. y GILS, T., «Tort law and damage caused by AI systems», en De Bruyne, J./Vanleenhove, C., *Artificial Intelligence and the Law*, Intersentia, Cambridge, 2021, p. 364.

⁵⁸ Propuesta de Directiva del Parlamento europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, 28.9.22 (COM/2022/495 final). Aprobación en primera lectura mediante «Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento 12.10.2023 - [COM (2022)0495 - C9-0322/2022 - 2022/0302(COD)].

⁵⁹ Propuesta de Directiva del Parlamento europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), 28.9.22 (COM/2022/496 final). Esta iniciativa viene a sustituir la Propuesta de Reglamento del PE recogida en la Resolución de 20 octubre de 2020 con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial [2020/2014(INL)], disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html, que representa la primera tentativa de regulación de la responsabilidad civil por daños causados por la inteligencia artificial en la UE, que no fue finalmente tramitada. Y ello porque, como digo, la CE decidió apartarse de las recomendaciones del PE, impulsando la aprobación de una directiva, en vez de un reglamento, que además es de mínimos.

⁶⁰ La última noticia que tengo al respecto es la publicación, en septiembre de 2024, del Informe de evaluación de impacto complementaria sobre la PDRIA, realizado por PHILIPP HACKER a petición de la Unidad de Evaluación de Impacto Ex-ante de la Dirección de Evaluación de Impacto y Prospectiva, dentro de la Dirección General de Servicios de Investigación Parlamentaria (EPRS) de la Secretaría del Parlamento Europeo (*Study about Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence. Complementary impact assessment*, disponible solo en inglés en [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU\(2024\)762861_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf)

En este estudio, se sugieren diferentes modificaciones en la regulación contenida en la PDRIA, empezando por la sustitución del instrumento legislativo que ha elegido la CE, una directiva, por un reglamento, como ya propuso el PE en 2020. Según HACKER, ello evitaría la fragmentación del mercado, aumentaría la claridad y fomentaría la innovación y la protección de los consumidores al establecer normas jurídicas coherentes en todo el mercado único digital. Esta opción, además, se ajustaría a las tendencias actuales de la legislación sobre seguridad de los productos, en la que numerosas directivas están siendo sustituidas por reglamentos (por ejemplo, el Reglamento sobre seguridad general de los

En efecto, la UE es consciente de que la dificultad para determinar la relación de causalidad puede derivar en un grado de resarcimiento menor en los pleitos por daños causados por sistemas inteligentes que en aquellos en los que la causa del daño sea otra; lo cual puede provocar un menor nivel de aceptación social de la IA y de confianza en los productos y servicios basados en ella⁶². Ante el temor de que los órganos jurisdiccionales nacionales adapten las normas vigentes a las características específicas de la IA para lograr la justicia en el caso concreto, con la consiguiente inseguridad jurídica que ello implicará para las empresas⁶³, así como de que los legisladores nacionales de los EEMM adopten sus propias regulaciones al respecto, provocando una mayor fragmentación y un aumento de los costes para las empresas que operan en la UE, esta ha tomado cartas en el asunto. Así, las propuestas de directiva de 2022 adoptan medidas para facilitar el acceso de los demandantes a las pruebas y aligerar la carga de la prueba que pesa sobre ellos, estableciendo ciertas presunciones *iuris tantum* de existencia de un defecto en el producto y/o del nexo de causalidad entre el defecto y el daño (en el caso de la PRDCPD) y de causalidad entre la culpa del demandado y el resultado dañoso generado por el sistema inteligente (en la PDRIA). Ahora bien, en mi opinión tales presunciones no mejorarán tanto como se esperaba la situación de los perjudicados en un pleito respecto a la carga de la prueba, porque en el afán por proteger a las víctimas sin frenar el desarrollo de la IA, los requisitos de aplicación de aquellas son, en ocasiones, demasiado exigentes, y en gran medida, se limitan a los sistemas de alto riesgo. Cabe recordar, además, que en el ordenamiento jurídico español ya disponemos de mecanismos para facilitar carga de la prueba, como los principios de disponi-

productos o el Reglamento sobre productos sanitarios). Por consiguiente, aboga por un Reglamento revisado sobre responsabilidad por productos defectuosos y un Reglamento sobre responsabilidad por IA (o más bien: un Reglamento sobre responsabilidad por *software*) en lugar de directivas.

⁶¹ La regulación prevista en ambas directivas pretende complementar la del Reglamento de IA, que, con un objetivo de prevención de daños, aborda los riesgos de posibles sesgos, errores y opacidad que pueden afectar negativamente a los derechos fundamentales y establece requisitos obligatorios para el diseño y desarrollo de sistemas inteligentes antes de su comercialización (MARTÍN CASALS, M., «Desarrollo tecnológico...», cit., p. 119). En la medida en que, como señala la E. de M. de la PDRIA, p. 3, las normas del Reglamento no eliminarán los riesgos por completo, las reglas recogidas en las proyectadas directivas permitirán que las víctimas obtengan resarcimiento cuando, a pesar de los requisitos preventivos del RIA y otras normas de seguridad, se produzcan daños; sin perjuicio de que las propuestas de Directiva contribuirán, asimismo, a prevenir los daños, ya que unas normas eficaces en materia de responsabilidad también ofrecen un incentivo económico para cumplir las normas de seguridad.

Las principales diferencias entre ambas Propuestas de Directiva se recogen en HACKER, P., *Study about...*, cit., p. 2.

⁶² Cdo. 4. DPRIA.

⁶³ En efecto, según se apunta en la E. de M. de la PDRIA, p. 3, las empresas, sobre todo las que se dedican al comercio transfronterizo, tendrán dificultades para predecir cómo se aplicarán las normas de responsabilidad civil vigentes y, por tanto, para evaluar y asegurar su exposición a dicha responsabilidad; lo cual «[a]fectará especialmente a las pymes, que no pueden recurrir a los conocimientos de servicios jurídicos propios ni cuentan con reservas de capital».

bilidad y facilidad probatoria recogidos en el art. 217.7 Ley de Enjuiciamiento Civil 1/2000 (LEC), las presunciones legales y judiciales (arts. 385 y 386 LEC) y la regla *res ipsa loquitur*, que se viene utilizando por los tribunales (con habitualidad en el ámbito sanitario) tanto para deducir la negligencia cuando las circunstancias conocidas son tales que no parece posible otra explicación del accidente que una negligencia en la esfera del demandado, que había estado en pleno control del incidente que pudo causar el daño, como para presumir la existencia de un defecto o de la relación de causalidad. De todo ello me ocupo con detalle en otro trabajo, al cual me remito⁶⁴.

Las dificultades para determinar la causa del daño complican, como es obvio, la del sujeto responsable. En efecto, por centrarnos en el ámbito sanitario, no es lo mismo que el daño sea consecuencia de la pérdida de control del aparato o de la incorrecta utilización del facultativo, de la ausencia de una actualización a una versión superior del sistema, de una falta de mantenimiento por el hospital, de un acontecimiento externo (como un ataque informático o una avería en el suministro de energía) o de una causa desconocida. Incluso las causas pueden derivar de una interacción de agentes (ingeniería mecánica, electrónica, tecnología de la información y *software* incorporado)⁶⁵.

Pues bien, las vías posibles para lograr una indemnización por daños causados por sistemas inteligentes son diferentes según las circunstancias y el sujeto frente al que se pretenda la indemnización. A determinarlas se dedican las páginas siguientes, teniendo en cuenta que puede recurrirse a más de una respecto del mismo daño, y advirtiendo que no se pretende desarrollar de forma exhaustiva los regímenes aplicables, sino tratar de aclarar cuándo se puede recurrir a cada uno de ellos y cuál es el fundamento de la responsabilidad que contemplan.

Voy a referirme, concretamente, a los regímenes especiales de responsabilidad civil objetiva contemplados en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre (en adelante, TRLGDCU), a saber: el relativo a daños causados por productos defectuosos

⁶⁴ EVANGELIO LLORCA, R., «Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 549-620. Ver, asimismo, HACKER, P., *Study about...*, cit., donde se proponen modificaciones respecto de la regulación contenida en la PDRIA respecto de la exhibición de pruebas y la presunción refutable de causalidad.

⁶⁵ EBERS, M., «La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?», *InDret*, 3/2106, p. 7; MONTERROSO CASADO, E., «Responsabilidad civil por daños causados por robots en el ámbito sanitario», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramientos*, dir. por Monterroso Casado, E. y coord. por Muñoz Villarreal, A., Tirant lo Blanch, Valencia, 2019, pp. 107-108.

(arts. 135 a 146) y el referente a daños provocados por servicios sanitarios (art. 148)⁶⁶; a la responsabilidad patrimonial de la Administración sanitaria, regulada en los arts. 32 a 36 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP), y, en los aspectos procesales, en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP); y, por último, a los regímenes de responsabilidad civil recogidos en el Código Civil (en adelante, CC).

3. DAÑOS CAUSADOS POR LA INTELIGENCIA ARTIFICIAL COMO PRODUCTO DEFECTUOSO

3.1. ÁMBITO DE APLICACIÓN DEL RÉGIMEN DE RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS. LOS SISTEMAS INTELIGENTES COMO PRODUCTOS DEFECTUOSOS

En la actualidad, la responsabilidad civil por daños causados por productos defectuosos está regulada, en la UE, por la Directiva 85/374/CEE⁶⁷, que fue transpuesta al ordenamiento jurídico español por la Ley 22/1994, de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos. Esta última norma se encuentra hoy derogada y refundida en el TRLGDCU, cuyos arts. 135 a 146 recogen la regulación específica de esta materia.

Este régimen se verá afectado por la ya mencionada PDRDPD. No obstante, durante varios años la normativa vigente seguirá siendo de aplicación, ya que, por un lado, se prevé que desde la entrada en vigor de la nueva Directiva los EEMM dispongan de veinticuatro meses para la transposición (art. 22 de la Propuesta), así como que la Directiva 85/374/CEE -y, por tanto, las normas nacionales de incorporación- siga aplicándose a los productos introducidos en el mercado o puestos en servicio antes de esa fecha (art. 21 de la Propuesta).

Así las cosas, a continuación trataré de determinar si la IA encaja en el régimen actual de responsabilidad civil por productos defectuosos y cuáles son

⁶⁶ El TRLGDCU ofrece una tercera vía para reclamar por daños causados por bienes de consumo: la acción de indemnización de daños y perjuicios ejercitable al amparo del régimen de responsabilidad del empresario por falta de conformidad del bien, del contenido digital o del servicio digital con el contrato, previsto en los arts. 114 y ss. Esta regulación, no es aplicable, sin embargo, en el caso de daños causados por el uso de sistemas inteligentes en el ámbito sanitario, dado que únicamente se aplica a los contratos de compraventa, de obra o de suministro de contenidos o servicios digitales celebrados entre un consumidor o usuario y un empresario.

⁶⁷ Directiva del Consejo de 25 de julio de 1985 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85/374/CEE).

los cambios que a este respecto incorpora la PDRDPD, que son numerosos y de relevancia⁶⁸; no en vano uno de los motivos que ha justificado la revisión de la Dir. 85/374/CEE ha sido proporcionar a los perjudicados una mejor protección frente a los nuevos riesgos que plantea la sociedad actual, entre los cuales ocupan un lugar preeminente los derivados de la IA⁶⁹.

3.1.1. El concepto de «producto» y la posible consideración del sistema inteligente como tal

En la actual regulación de la responsabilidad civil por daños causados por productos defectuosos, se duda si los SIA pueden ser considerados productos a los efectos de reclamar dicha responsabilidad; y ello porque, de acuerdo con el art. 136 TRLGDCU, procedente del art. 2 Dir. 85/374, «se considera producto cualquier bien mueble, aun cuando esté unido o incorporado a otro bien mueble o inmueble, así como el gas y la electricidad». El problema podría residir en la aplicación del concepto de producto a bienes intangibles, como el *software* que no está incorporado a un bien corpóreo; porque si lo está, como en el caso de los robots físicos, hay consenso en entender que el conjunto de la estructura física y el programa informático se considerará como un bien mueble y, por tanto, como producto⁷⁰.

⁶⁸ Tanto es así que se ha considerado que no era suficiente con modificar la Directiva de 1985, sino que era necesario derogarla y sustituirla por una nueva (cdo. 5 PDRDPD).

⁶⁹ Ciertamente, no es esta la única razón que ha dado lugar a la PDRDPD, sino que obedece también, como pone de relieve HERBOSA MARTÍNEZ, I., «Encaje de...», cit., p. 60, a la necesidad de revisar algunas reglas o provisiones generales relativas a la exoneración del productor por riesgos del desarrollo (sobre lo que se viene debatiendo desde la adopción de la directiva), la extensión de los daños indemnizables y la cobertura de los ocasionados a personas que no sean consumidores; pero sí ha sido, como decía, la principal. En este sentido, en su Informe de 2018 de evaluación de la Dir. 85/374/CEE, la CE declaraba que «los problemas a los que nos enfrentamos en la actualidad difieren en cierta medida de los que existían en el mundo predominantemente analógico de 1985. Nos encontramos inmersos en otra revolución tecnológica. La economía y los propios productos están aumentando gradualmente su interconexión, su digitalización, su autonomía y su inteligencia. Necesitamos una respuesta coherente y global ante estos retos, tal como se describe en la iniciativa sobre inteligencia artificial» [COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre la aplicación de la Directiva del Consejo relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85/374/CEE)], 7 mayo 2018, disponible en <https://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52018DC0246&from=FR>.

⁷⁰ Ver, entre otros: DÍAZ ALABART, S., *Robots y responsabilidad civil*, Reus, Madrid, 2018, pp. 100-101; MONTERROSO CASADO, E., «Responsabilidad civil...», cit., p. 112; ZURITA MARTÍN, I., *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020, pp. 82-84, y «Las propuestas de...», cit., p. 459; KOCH, B., BORGHETTI, J. S., MACHNIKOWSKI, P., PICHONNAZ, P., RODRÍGUEZ DE LAS HERAS BALLELL, T., TWIGG-FLESNER, C., WENDEHORST, C., *Response of the...*, cit.; NAVAS NAVARRO, S., «Responsabilidad civil

Pues bien, en mi opinión, que coincide con la de gran parte de la doctrina⁷¹, hay argumentos más que suficientes para entender que también cuando no tengan un soporte material, los programas de ordenador pueden considerarse productos a los efectos del régimen de responsabilidad por daños causados por productos defectuosos⁷². No obstante, es loable que la PDRPD haya ampliado el concepto de producto para incluir expresamente en él los programas informáticos (art. 4.1), y como un tipo de ellos, los sistemas inteligentes⁷³. Es interesante recalcar, además, que la consideración de los programas informáticos como productos a efectos de la aplicación de la responsabilidad objetiva se hace «independientemente de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo, se accede a él a través de una red de comunicaciones o tecnologías en la nube o se suministra a través de un modelo de programa informático como servicio»⁷⁴.

Mas no todos los programas informáticos quedan incluidos en el concepto de producto, ya que se excluyen expresamente los que sean libres y de código abierto que se desarrollen o suministren fuera del transcurso de una actividad comercial quedan excluidos del concepto de producto (art. 2.2, modificado en la última versión de la Propuesta⁷⁵). Ahora bien, el cdo. 15 dispone que

del fabricante y tecnología inteligente», *la Ley*, núm. 35, sección Ciberderecho, 27 diciembre 2019, p. 2; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., pp. 141-142, y «¿Una nueva...» cit., p. 7; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 147; GARCÍA MICÓ, T. G., *Robótica quirúrgica y Derecho de daños*, Marcial Pons, Madrid, 2024, p. 65.

⁷¹ ATAZ LÓPEZ, J., «Daños causados...», cit., p. 35; ZURITA MARTÍN, I., *La responsabilidad civil...*, cit., pp. 85-87, y «Las propuestas de...», cit., p. 459; RAMÓN FERNÁNDEZ, F., «Inteligencia artificial...», cit., p. 344; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., pp. 142-145, y «¿Una nueva...», cit., p. 7; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., pp. 151 y ss.; HERBOSA MARTÍNEZ, I., «Encaje de...», cit., p. 68; GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., p. 66.

⁷² Recogidos por ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., pp. 143-144, y «¿Una nueva...», cit., pp. 7-8.

⁷³ En efecto, el cdo. 13 incluye específicamente como tipos de programas informáticos los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones y los sistemas de inteligencia artificial.

⁷⁴ La diferencia entre el *software* como bien o como servicio debe establecerse, según HERBOSA MARTÍNEZ, I., «Encaje de...», cit., p. 90, en función del modelo de distribución; así, estaremos ante *software* como bien cuando el programa se instala en el equipo del usuario, mientras que se tratará de un servicio cuando no requiere instalación en el equipo del usuario, sino que aquel se aloja en los servidores del proveedor (o de terceros). «De este modo, el sistema de IA se pone a disposición del usuario, pero sin necesidad de que este tenga que invertir en su instalación, en equipos o servidores de su propiedad, lo que le permite cubrir sus necesidades de una forma más ágil y económica que con otras formas de acceso al mismo».

⁷⁵ La justificación de la exclusión es, según la CE, no obstaculizar la innovación o la investigación, unido al hecho de que los productos así desarrollados o suministrados no se comercializan (cdo. 14). Este segundo motivo ha sido añadido por el PE en su primera lectura y debe considerarse el principal, porque el de no obstaculizar la innovación o la investigación no es demasiado convin-

«[c]uando los programas informáticos libres y de código abierto suministrados al margen de una actividad comercial sean posteriormente integrados por un fabricante como componente en un producto en el transcurso de una actividad comercial y, por tanto, se introduzcan en el mercado, debe ser posible considerar a dicho fabricante responsable de los daños causados por el carácter defectuoso de dichos programas, pero no así al fabricante de los programas puesto que no habría reunido las condiciones de comercialización de un producto o componente».

En segundo lugar, cabe reparar en la inclusión como producto de los bienes muebles que estén interconectados con otros bienes muebles o inmuebles.

La Propuesta define otro concepto importante en relación con la IA: el de «componente», esto es, «cualquier artículo, tangible o intangible, o materia prima, o cualquier servicio conexo, que está integrado en un producto o interconectado con él» (art. 4.4). A estos efectos, por «servicio conexo» se entiende «un servicio digital que está integrado en un producto o interconectado con él, de tal manera que su ausencia impediría al producto realizar una o varias de sus funciones» (art. 4.3); por ejemplo, un servicio de vigilancia de la salud que se basa en sensores de un producto físico para rastrear la actividad física o los parámetros de salud del usuario (cdo. 17 PDRDPD⁷⁶).

En la regulación vigente no se hace referencia a la categoría de componente de un producto, pero sí al equivalente de «parte integrante» de un producto acabado (art. 3 Dir. 85/374/CEE) o «elemento» de un producto terminado (art. 138 TRLGDCU) que se considera como un producto en sí mismo⁷⁷. En relación con ello, y a falta de mención expresa, cabe preguntarse si en el régimen actual los servicios conexos pueden considerarse parte integrante o elemento del SIA a efectos de responsabilidad por daños causados por productos defectuosos. Entiendo, con HERBOSA MARTÍNEZ, que sí, puesto que entre «todas las circunstancias» que deben tomarse en consideración para determinar el carácter defectuoso de un producto están los servicios que, al hallarse integrados o interconectados con el bien, afecten a alguna o

cente (en este sentido, GÓMEZ LIGÜERRE, C., «Responsabilidad del prestador de servicios por daños causados por productos defectuosos», *RDP*, julio-agosto 2009, p. IV, y ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 9).

⁷⁶ En relación con ello, el citado considerando explica que «[a]unque la presente directiva no debe aplicarse a los servicios como tales, es necesario ampliar la responsabilidad objetiva a tales servicios digitales, ya que determinan la seguridad del producto tanto como los componentes físicos o digitales».

⁷⁷ Como recuerda HERBOSA MARTÍNEZ, I., «Encaje de...», cit., p. 72, que cita la STS 649/3014 (Sala Civil), de 13 de enero de 2015 (Roj: STS 181/2015), que ha considerado como producto defectuoso el *software* dotado de inteligencia artificial incorporado a un avión causante del accidente en el que se vio implicado este.

varias de sus funciones⁷⁸. Entre estos servicios deben incluirse, asimismo, los datos suministrados para el funcionamiento del SIA en el marco de una prestación de servicios.

En otro orden de cosas, la diferencia entre producto y componente de un producto que realiza la Propuesta es aplicable a los sistemas inteligentes, los cuales pueden ser productos -lo que la CE ha denominado «IA como *software*», cuando funcionan desvinculados de cualquier soporte material o físico (asistentes virtuales, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento de voz y rostro, etc.); o bien pueden comercializarse integrados en otros bienes (robots, drones, vehículos autónomos, Internet de las Cosas, etc.), dando lugar a lo que la CE conoce como «IA integrada» y que, a los efectos del régimen por daños causados por productos defectuosos, se considerará como un componente de un producto⁷⁹; sería el caso, como apunta GARCÍA MICÓ, de un programa informático instalado en una máquina de rayos X que transforma los datos captados por la interacción entre los imanes adheridos al paciente y el campo de radiación generado por la máquina de TRM (tomografía por resonancia magnética) en una imagen que pueda ser captada y comprendida por su destinatario⁸⁰.

3.1.2. Un tipo específico de producto: el producto sanitario

En la categoría de productos, a los efectos del régimen de responsabilidad civil por daños causados por productos defectuosos recogido en el TRLGDCU, se incluyen los denominados «productos sanitarios», los «accesorios de productos sanitarios» y otros productos que, aun sin perseguir fines médicos, se encuentran relacionados con los anteriores.

Todos ellos vienen regulados por el Reglamento (UE) 2017/745 de productos sanitarios (en adelante, RPS)⁸¹, cuyo art. 2.1 define el «producto sani-

⁷⁸ HERBOSA MARTÍNEZ, I., «Encaje de...», cit., p. 89.

⁷⁹ PARLAMENTO EUROPEO, *¿Qué es la inteligencia artificial y cómo se usa?*, 26 marzo 2021, disponible en https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804/20200827STO85804_es.pdf. GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., pp. 66-67, por su parte, distingue entre el *software* como producto sanitario (SaMD, *Software as a Medical Device*) y el *software* como componente de un producto sanitario (SiMD, *Software in a Medical Device*).

⁸⁰ GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., p. 67.

⁸¹ Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) núm. 178/2002 y el Reglamento (CE) núm. 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo. El objetivo de este Reglamento es establecer normas relativas a la introducción en el mercado, la comercialización o la puesta en servicio de productos sanitarios para uso humano y accesorios de dichos productos en la UE, a las investigaciones clínicas

tario» como «todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos: diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad; diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad; investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico; obtención de información mediante el examen *in vitro* de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos, y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos».

El precepto añade que también se consideran productos sanitarios los productos de control o apoyo a la concepción, así como los productos destinados específicamente a la limpieza, desinfección o esterilización de aquellos y de los productos sanitarios contemplados en el art. 1.1) a los que se acaba de hacer referencia.

Los productos sanitarios se clasifican en clase I, IIa, IIb y III, conforme a las reglas establecidas en el Anexo VIII del RPS, y esta clasificación es importante a efectos de la «evaluación de conformidad»⁸² a la que los productos sanitarios y sus accesorios deben someterse antes de introducirse en el mercado, comercializarse o usarse en servicios sanitarios⁸³. Hay que tener en cuenta, además, que cuando el producto sanitario tenga como función suministrar un medicamento, no solo estará sujeto a los controles propios de los productos sanitarios, sino también a los propios de los medicamentos en los términos del art. 1.9 del Reglamento⁸⁴.

relativas a los productos sanitarios y accesorios que se llevan a cabo en la Unión, y a ciertos productos que no persiguen fines médicos y que vienen recogidos en el Anexo XVI de la norma (art. 1).

⁸² Definida en el art. 2.40) Reglamento (UE) 2107/745 como «el proceso por el que se demuestra si un producto satisface los requisitos del presente Reglamento».

⁸³ GRIMALT SERVERA, P., «La responsabilidad (civil o patrimonial) del personal médico, de los centros sanitarios y de las administraciones sanitarias por los daños causados por un producto sanitario defectuoso», *Bioderecho.es*, núm. 17, enero-julio 2023, p. 4. Como señala este autor, el Reglamento distingue también entre diferentes tipos de productos sanitarios (producto a medida, producto activo, producto implantable, producto invasivo, producto de un solo uso), que resultan sometidos a distintos tipos de control y garantías para que se autorice su comercialización y uso posterior por parte de pacientes. Esto podría tener incidencia a los efectos de imputar o exonerar responsabilidad al servicio de salud que los ha utilizado.

⁸⁴ Así lo apunta también GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 6. Además de a la evaluación de conformidad prevista en el RPS, los productos sanitarios están sujetos al control de seguridad *ex ante* del RIA, lo cual genera inquietud en las empresas del sector, debido a que el tener que pasar por dos evaluaciones de conformidad puede conducir a que cuando el producto esté

Por su parte, un «accesorio de un producto sanitario» se define, a los efectos del RPS, un «accesorio de un producto sanitario» es «un artículo que, sin ser en sí mismo un producto sanitario, está destinado por su fabricante a ser usado de forma conjunta con uno o varios de dichos productos, para permitir específicamente que el producto o productos sanitarios puedan utilizarse con arreglo a su finalidad prevista o para contribuir específica y directamente a la funcionalidad médica de los productos sanitarios a efectos de su finalidad prevista» (art. 2.2).

En lo que aquí interesa, tanto en el concepto de producto sanitario como en el de accesorio de un producto sanitario a los efectos del RPS pueden tener cabida, dada la amplitud con la que se definen estos conceptos, los sistemas inteligentes⁸⁵.

Finalmente, los productos sin finalidad médica recogidos en el Anexo XVI del Reglamento son los siguientes: 1. Lentes de contacto u otros artículos destinados a ser introducidos o colocados en el ojo; 2. Productos destinados a ser total o parcialmente introducidos en el cuerpo humano mediante medios invasivos de tipo quirúrgico a efectos de modificación de la anatomía o fijación de partes del cuerpo, con excepción de los productos para tatuajes y piercings; 3. Sustancias, combinaciones de sustancias o artículos destinados a su uso como relleno facial o en otras zonas dérmicas o de membranas mucosas mediante inyección subcutánea, submucosa o intradérmica o con otros medios de introducción, excluidos los destinados al tatuaje; 4. Equipos destinados a usarse para reducir, retirar o destruir tejido adiposo, como los equipos para liposucción, lipólisis o lipoplastia; 5. Equipos que emiten radiación electromagnética de alta intensidad (por ejemplo, infrarrojos, luz visible y ultravioleta) destinados a su uso en el cuerpo humano, con inclusión de fuentes coherentes y no coherentes, monocromáticas o de amplio espectro, tales como láseres y equipos de luz pulsada intensa para rejuvenecimiento de la piel, eliminación de tatuajes, depilación u otros tratamientos dérmicos; 6. Equipos destinados a la estimulación cerebral que aplican corrientes eléctricas o campos magnéticos o electromagnéticos que penetran en el cráneo para modificar la actividad neuronal del cerebro.

En otro orden de cosas, de acuerdo con el art. 101 del Reglamento (UE) de productos sanitarios, los estados miembros deben designar una autoridad competente para hacer cumplir con lo previsto en el referido Reglamento, que

listo para ponerlo en el mercado, ya sea obsoleto (CASTELLÓ, I., «Seguridad de los sistemas de IA en salud», ponencia presentada en el *I Congreso Internacional Digitalización e Inteligencia Artificial en la contratación y prestación de servicios médicos*, UPNA, Pamplona, 4 de octubre de 2024).

⁸⁵ Ver, a este respecto, LUQUIN BERGARECHE, R., «Responsabilidad contractual...», cit., pp. 304 y ss.

en España es la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS), de acuerdo con lo previsto en el art. 4 del Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios⁸⁶. Este control previo de los productos sanitarios por parte de la AEMPS tendrá, como pone de relieve GRIMALT SERVERA, una relevancia decisiva para excluir la responsabilidad patrimonial de las Administraciones sanitarias públicas (o civil cuando se trate de servicios o centros sanitarios privados) cuando dichos productos no funcionen correctamente y causen un daño en los pacientes que hagan uso de aquellos⁸⁷.

En España, además de los citados Reglamentos UE, los productos sanitarios vienen regulados por el RD Legislativo 1/2015, de 24 de julio, por el que se aprueba el Texto Refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios⁸⁸, el RD 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios, en las partes que no han sido derogadas (precisamente por la aprobación de la citada normativa comunitaria) por el Real Decreto 192/2023, de 21 de marzo.

En lo que a la responsabilidad civil se refiere, los daños causados por productos sanitarios, accesorios de productos sanitarios y productos sin finalidad médica contemplados en el RPS que sean defectuosos quedan sometidos al régimen de la Directiva 85/374/CE y, en España, de los arts. 135 y ss. TRLGDCU, así como al proyectado por la PDRCPD⁸⁹.

3.1.3. «Productos defectuosos», «componentes defectuosos» y sistemas inteligentes

En cuanto al concepto de producto defectuoso, de conformidad con el vigente art. 137.1 TRLGDCU, es «aquél que no ofrezca la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razonablemente previsible del mismo y el momento de su puesta en circulación»⁹⁰. La redacción del precepto es prácticamente la misma

⁸⁶ No obstante, en algunos casos, la evaluación de conformidad la realiza el propio fabricante a través de una declaración, como en el caso del art. 52.7 RPS, como destaca GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 6.

⁸⁷ GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 5.

⁸⁸ Respecto de la diferencia entre medicamentos y productos sanitarios ver ÁLVAREZ OLALLA, P., «Daños causados al paciente por utilización de un producto sanitario defectuoso. Al hilo del caso Ala Octa», *RCDI*, núm. 794, 2022, p. 3368.

⁸⁹ Sin perjuicio del régimen sancionador por infracciones en materia de productos sanitarios previsto en el art. 112 del Texto Refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios de 2015.

⁹⁰ Tal y como recuerdan las SSTJUE 5 marzo 2015, C-503/13 y C-504/13, Boston Scientific Medizintechnik, ECLI:EU:C:2015:148, y 10 junio 2021, C-65/20, Krone, ECLI:EU:C:2021:471, el cdo.

que la del art. 6 Dir. 85/374/CEE, con la única diferencia de que este se refiere a la seguridad «a la que una persona tiene legítimamente derecho».

El art. 7 PDRPD, por su parte, dispone que «[u]n producto se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional». En cuanto a los criterios que deben tenerse en cuenta para evaluar si se da o no esa seguridad, al igual que la vigente directiva, se alude a «todas las circunstancias», mencionando expresamente las siguientes, entre las que se incluyen las que ya recoge la normativa vigente y otras que se han añadido: a) la presentación y las características del producto, incluidos su etiquetado, diseño, características técnicas, composición y envase, y las instrucciones de montaje, instalación, uso y mantenimiento⁹¹; b) el uso razonablemente previsible del producto; c) el efecto en el producto de la posibilidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio; d) el efecto razonablemente previsible sobre el producto de otros productos que queden a la espera de que se utilicen junto con el producto, también mediante interconexión; e) el momento en que el producto fue introducido en el mercado o puesto en servicio o, si el fabricante conserva el control sobre el producto después de ese momento, el momento en que el producto dejó el control del fabricante; f) los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad pertinentes para la seguridad⁹²; g) cualquier retirada del producto o cualquier intervención pertinente de una autoridad competente o de un operador económico contemplado en el artículo 8 en relación con la seguridad de los productos; h) las necesidades específicas del grupo de usuarios finales a los que se destina el producto; i) en el caso de un producto cuya finalidad es precisamente evitar daños, el eventual incumplimiento de dicha finalidad por parte del producto.

Este listado de circunstancias no debe considerarse exhaustivo, sino que deberá complementarse, en su caso, cuando se trate de sistemas de IA de alto riesgo, con lo establecido en el RIA en cuanto a requisitos de seguridad y obligaciones exigibles a los diferentes sujetos⁹³.

6 de la Directiva 85/374 señala que las expectativas de seguridad que deben tenerse en cuenta son las del gran público.

⁹¹ En relación con los sistemas de IA, el art. 3.15) RIA define como «instrucciones de uso: la información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA».

⁹² Así, como destaca GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., pp. 107-108, el riesgo de hackeo de un sistema inteligente será un defecto de diseño que convertirá a este en un producto defectuoso.

⁹³ JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 186.

Por lo que se refiere al nivel de seguridad esperable, la doctrina plantea una interesante cuestión respecto de los SIA, y es la de qué seguridad cabe esperar de ellos. Partiendo de la base de que, en general, y también por tanto cuando hablamos de la intervención de sistemas inteligentes, las exigencias de seguridad deben ser mayores cuanto más elevado sea el bien jurídico que puede verse amenazado⁹⁴, y que, por tanto, en el campo de la medicina las exigencias serán altas, la pregunta es si cabe exigir mayor seguridad a los SIA que a los humanos. Por ejemplo, si hablamos de cirugías de columna vertebral, en las que la cirugía convencional supone un riesgo en torno al 15 o 20% de malposición de prótesis, ¿qué riesgo vamos a aceptar en la cirugía robótica? ¿El mismo que en la cirugía convencional? ¿La mitad? ¿O quizá un vamos a exigir un 0% de riesgo?⁹⁵. Sin llegar a tanto, algunos autores se decantan por entender que la exigencia de seguridad exigible a un robot quirúrgico debe ser más elevada que la exigible a cirujanos humanos⁹⁶.

En relación con el concepto de defecto, cabe plantearse si es posible considerar como tales las decisiones o recomendaciones inexactas generadas por un SIA cuando son dichos resultados los que causan un daño (como sería el caso de un diagnóstico erróneo). HERBOSA MARTÍNEZ sostiene que no, basando su opinión en la STJUE de 10 junio 2021, C-65/20, KRONE c. Verlag Gesellschaft mbH & Co KG⁹⁷. En ella, se declara que no constituye producto defectuoso un ejemplar de periódico impreso en el que, tratando de un tema paramédico, se incluye un consejo de salud inexacto relativo a la utilización de una planta (rábano recién rallado), cuyo seguimiento por un lector causa daños a su salud. Como indica la citada autora, a juicio del TJUE lo que en este caso es defectuoso es el consejo, que en sí mismo tiene la consideración de servicio, y que en todo caso no forma parte de los elementos intrínsecos del periódico impreso, pues no se refiere a la presentación ni al uso de este, que son los únicos que permiten apreciar si dicho producto es defectuoso.

Pues bien, trasladando este razonamiento a los sistemas de IA, HERBOSA MARTÍNEZ sostiene que no cabe imponer responsabilidad al proveedor de los mismo por los daños que ocasione la información defectuosa que generen dichos sistemas, si dicha información no tiene un reflejo en el comportamiento, utilidades y/o presentación del propio sistema o del bien en el que

⁹⁴ EBERS, M., «La utilización...», cit., p. 11.

⁹⁵ En estos términos lo plantean MUÑOZ VILLARREAL, A. y GALLEGU CORCHERO, V., «Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad de los robots», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramientos*, dir. por Monterroso Casado, E. y coord. por Muñoz Villarreal, A., Tirant lo Blanch, Valencia, 2019, p. 90.

⁹⁶ MONTERROSO CASADO, E., «Responsabilidad civil...», cit., p. 115.

⁹⁷ ECLI:EU:C:2021:471.

se integra este; lo cual la lleva a concluir que los sistemas de IA generativa, como *ChatGPT*, se deben considerar excluidos del ámbito de aplicación de la normativa de productos defectuosos.

A mi entender, en cambio, entre el caso resuelto por la citada STJUE y el supuesto de la IA generativa hay una diferencia fundamental: en la situación resuelta por la sentencia, el periódico es un mero soporte y el consejo es un servicio; en una herramienta de diagnóstico, por ejemplo, por el contrario, el diagnóstico forma parte de la funcionalidad del *software* que lo emite. Por consiguiente, creo que sí quedarán cubiertos los daños causados por las decisiones de los sistemas inteligentes.

Por otro lado, en relación con los productos sanitarios, cabe indicar que la falta de seguridad puede darse con independencia de que el producto cuente o no con las autorizaciones pertinentes para su fabricación y comercialización, así como de que cumpla las prescripciones que le sean aplicables⁹⁸.

En otro orden de cosas, la vigente normativa concibe el producto defectuoso de manera estática, de modo que una vez puesto en circulación por el fabricante está acabado totalmente y no será objeto de mejoras ni adaptaciones por su parte; de ahí que ese momento sea tomado como referencia para determinar la existencia del defecto y de algunas causas de exoneración o marque el *dies a quo* para el cómputo de los plazos de prescripción y preclusión⁹⁹.

Ello no encaja bien con los sistemas inteligentes. Por esta razón, la PDRDPD fija como momento que debe tenerse en cuenta para determinar el carácter defectuoso, como se ha visto, aquel «en que el producto fue introducido en el mercado o puesto en servicio o, si el fabricante conserva el control sobre el producto después de ese momento, el momento en que el producto dejó de estar bajo el control del fabricante» [art. 7.2 e)]. El concepto de «puesta en servicio» es especialmente útil, como afirma el cdo. 26 de la Propuesta, tras la adición realizada por el PE en primera lectura, respecto de los productos que no se comercializan antes de su primera utilización, como puede ocurrir en los sectores de los ascensores, la maquinaria o los productos sanitarios.

Por otra parte, en relación con los SIA, son muy interesantes otros factores a los que, según el art. 7 de la Propuesta, deberá atenderse a la hora de

⁹⁸ GIL MEMBRADO, C., *La responsabilidad civil por implante mamario. Mala praxis, consentimiento informado y prótesis defectuosa*, Comares, Granada, 2014, p. 138; LÓPEZ TUR, T., «Producto defectuoso e impresión de prótesis con impresoras 3D», en *Derecho y medicina: desafíos tecnológicos y científicos*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2023, p. 51.

⁹⁹ PACHECO CAÑETE, M., «Reflexiones sobre la responsabilidad civil del empresario por los daños causados por sistemas de inteligencia artificial: situación actual y perspectivas futuras», *RGLJ*, 2023, núm. 2, pp. 297-298.

evaluar el carácter defectuoso, a saber: el efecto en el producto de la posibilidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio [art. 7.2.c)]; el efecto razonablemente previsible sobre el producto que otros que quepa esperar que se utilicen junto con aquel, también mediante interconexión [art. 7.2.d)]; los requisitos de seguridad del producto pertinentes, incluidos los de ciberseguridad pertinentes [art. 7.2.f)].

En cuanto al primero, tiene que ver con la cuestión de si se debe responder por los daños causados por un sistema inteligente cuando actúa de una manera no prevista inicialmente, que algunos autores ponen sobre la mesa en relación con la regulación vigente¹⁰⁰. A este respecto, un sector doctrinal estima que es dudoso que en el caso de los dispositivos que incorporan la característica del autoaprendizaje se deban calificar como «defecto» las decisiones erróneas, puesto que dichos sistemas necesariamente dan lugar a desviaciones impredecibles en la toma de decisiones, «lo que significa que en el diseño va implícita la posibilidad de una decisión errónea, la cual es, sin embargo, necesaria para el aprendizaje del dispositivo»¹⁰¹; mientras que otro, más tajantemente, sostiene que la peligrosidad de un producto, cuando es conocida por el público, no puede considerarse un defecto porque no existen expectativas de seguridad que puedan verse frustradas¹⁰²; y propone ampliar la noción de defecto para abarcar también los supuestos de productos no defectuosos en sí mismos, pero sí peligrosos, entre los que tiene cabida la IA fuerte¹⁰³. Pues bien, en esta línea apunta la Propuesta, a mi modo de ver, como corrobora el cdo. 32, que declara que existe una «expectativa legítima de que el programa informático de un producto y los algoritmos subyacentes estén diseñados de manera que se evite un comportamiento peligroso del producto», por lo que «un fabricante que diseñe un producto con la capacidad de desarrollar un comportamiento inesperado debe seguir siendo responsable de todo comportamiento que cause daños»¹⁰⁴.

¹⁰⁰ MUÑOZ VILLARREAL, A. y GALLEGO CORCHERO, V., «Inteligencia artificial...», cit., p. 90.

¹⁰¹ ATAZ LÓPEZ, J., «Daños causados...», cit., p. 38, a quien sigue ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 17.

¹⁰² NÚÑEZ ZORRILLA, M.^a C., «Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial», *Revista española de derecho europeo*, núm. 66, 2018, p. 32. También MONTERROSO CASADO, E., «Responsabilidad civil...», cit., p. 116, destaca que no puede confundirse producto peligroso con defectuoso.

¹⁰³ NÚÑEZ ZORRILLA, M.^a C., «Los nuevos retos...», cit., pp. 32-33. En el mismo sentido, MONJE BALMASEDA, Ó., «Robótica y responsabilidad en el ámbito sanitario», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, p. 452, sostiene que «no cabe sino la apuesta clara y sin matices por la no exoneración de responsabilidad por la imprevisibilidad del acontecimiento».

¹⁰⁴ En opinión de HERBOSA MARTÍNEZ, I., «Encaje de...», cit., pp. 92-93, «el hecho de que el comportamiento concreto adoptado por el sistema de IA sea impredecible no impide que pueda

3.2. SUJETOS RESPONSABLES

3.2.1. Determinación de los sujetos responsables

El sujeto responsable, de acuerdo con la regulación vigente, es el productor, que, de la combinación de los arts. 5 y 138 TRLGDCU se deriva que puede ser:

1) El fabricante o el importador en la UE de un producto terminado, de cualquier elemento de un producto terminado o de una materia prima, así como a cualquier persona que se presente como tal al indicar en el bien, ya sea en el envase, el envoltorio o cualquier otro elemento de protección o presentación, o servicio su nombre, marca u otro signo distintivo.

En la medida en que, como se ha señalado, el software integrado en un producto debe tener la consideración de componente del mismo a los efectos del TRLGDCU, el programador ha de entenderse incluido en el concepto de fabricante¹⁰⁵.

2) El prestador del servicio o su intermediario. Esta previsión genera discrepancia en la doctrina: por un lado, hay quien la critica, a mi juicio con razón¹⁰⁶, mientras que, por otro, si bien se reconoce que el solapamiento de regímenes entre el de productos defectuosos y el de servicios resulta inadecuado, se ve con buenos ojos porque facilita la posible reclamación del perjudicado en un ámbito en el que en ocasiones resulta complejo determinar si el daño se originó como consecuencia del producto o del servicio¹⁰⁷.

apreciarse un defecto de diseño que dé lugar a la responsabilidad del fabricante, en tanto que el riesgo de que dicho sistema desarrolle un comportamiento de esta naturaleza es previsible. De igual modo, se rechaza que la autonomía, y por ende la imprevisibilidad constituya por sí mismo un defecto, de manera que el fabricante deba responder en todo caso, pues los resultados serían excesivos y no existe ninguna justificación para entenderlo así. Por tanto, teniendo en cuenta la capacidad de aprendizaje del sistema, las expectativas legítimas de seguridad consisten en que el sistema de IA esté diseñado de forma que no tenga la capacidad de desarrollar un comportamiento que sea imprevisible, bien entendido que el fabricante sólo responderá por defecto de diseño en caso de que este hubiese podido evitarse o anularse mediante un diseño alternativo razonable».

¹⁰⁵ GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., pp. 86-87.

¹⁰⁶ MARTÍN CASALS, M. y SOLÉ FELIU, J., «¿Refundir o legislar? Algunos problemas de la regulación de la responsabilidad por productos y servicios defectuosos en el Texto Refundido de la LGDCU», *Revista de Derecho privado*, núm. 92, 2008, pp. 85-87; GUTIÉRREZ DE SANTIAGO, P., *Daños causados por productos defectuosos*, Thomson Aranzadi, Cizur Menor (Pamplona), 2008, p. 174, para quien «representa una incongruencia con la esencia del régimen de responsabilidad civil y constituye un error de bulto»; CÁMARA LAPUENTE, S., *Comentarios a las normas de protección de los consumidores*, Colex, Madrid, 2011, pp. 169 y ss.; GALÁN CORTÉS, J. C., *Responsabilidad civil médica*, Civitas Thomson Reuters, 6ª ed., 2018, p. 484; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 202.

¹⁰⁷ CAYÓN DE LAS CUEVAS, J., *La prestación de servicios sanitarios como relación jurídica de consumo*, Civitas Thomson Reuters, Cizur Menor (Navarra), 2017, pp. 527-528. Y ello con más razón,

Más allá de discusiones doctrinales, lo cierto es que la CE, al menos en dos ocasiones, ha afirmado claramente que la Dir. 85/374/CEE solamente se aplica a los productos, sin que los servicios estén contemplados en ella¹⁰⁸. En la misma línea, el TJUE, en la Sentencia de la Gran Sala de 21 diciembre 2011, asuntos acumulados C-411/10 y C-493/10, *Centre Hospitalier Universitaire de Besançon c. Thomas Dutruex y otros*, relativa al uso de un colchón térmico defectuoso durante una intervención quirúrgica que produjo quemaduras al paciente sin que se apreciase culpa de los facultativos, descartó la posibilidad de que el hospital usuario del colchón pueda responder con base en la mencionada Directiva, ya que este supuesto queda al margen de ella¹⁰⁹. Por tanto, a mi modo de ver, la previsión del art. 5 TRLGDCU en el sentido de incluir en el concepto de productor al prestador del servicio, choca con las disposiciones de la Directiva y con la doctrina del Tribunal de Luxemburgo; no obstante, siguiendo una interpretación literal de la ley española, el centro sanitario que haya prestado asistencia a un paciente que haya sufrido un daño por el uso de un producto defectuoso, pongamos por caso un sistema inteligente, podrá ser responsable como productor, sin perjuicio de la acción de repetición frente al fabricante o importador *ex art.* 132 TRLGDCU¹¹⁰.

todavía, según este autor, por la limitación de la potencialidad del art. 148 TRLGDCU a los aspectos funcionales y organizativos por parte de la jurisprudencia, a la que más adelante me referiré.

¹⁰⁸ Así, como destaca CAYÓN DE LAS CUEVAS, J., *La prestación de...*, cit., p. 527, el Informe de la CE sobre la aplicación de la Directiva de 31 de enero de 2001 [COM (2000) 893 final], señala, en su apartado 3.2.8, que «la Directiva sólo se aplica a los productos»; y anteriormente, el Libro verde sobre la responsabilidad civil por productos defectuosos de 28 de julio de 1999 [COM (1999) 396 final] había afirmado que «los servicios defectuosos no están contemplados por la Directiva 85/374/CEE».

¹⁰⁹ En palabras de la citada sentencia, «ese usuario ni puede ser considerado como un participante en la cadena de fabricación y de comercialización del producto en cuestión a la que se asocia, como se acaba de recordar, el concepto de “productor” contenido en el artículo 3 de la Directiva 85/374 ni, por lo tanto (...) ser calificado como suministrador de dicho producto en el sentido del apartado 3 de este artículo». Estoy de acuerdo con esta posición, al igual que GÓMEZ LIGÜERRE, C., «Responsabilidad del...», cit. p. 77, quien apunta, a mi juicio acertadamente, que no cabe considerar proveedor al prestador de servicios que emplea un producto en el desarrollo de la actividad en que consiste el servicio, pero sin transmitirlo al consumidor ni incorporarlo al resultado final del servicio, o al menos no como el elemento típico que define el servicio. Y esto es lo que ocurre, precisamente, en su opinión, con los servicios sanitarios. En contra, PARRA LUCÁN, M.^a Á., «Responsabilidad civil por bienes o servicios defectuosos», en *Comentario del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias*, coord. por R. Bercovitz Rodríguez-Cano, 2^a ed., Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2015, p. 2087.

En la misma línea, la más reciente STJUE 10 junio 2021, C-65/20, *KRONE c. Verlag Gesellschaft mbH & Co KG*, ECLI:EU:C:2021:471, sobre responsabilidad por el daño causado por un consejo incluido en un periódico.

¹¹⁰ Así lo ponen de manifiesto CUETO PÉREZ, M., «Jurisprudencia en el caso ALA OCTA: responsabilidad patrimonial por la utilización de productos defectuosos en el ámbito sanitario», *Revista de Administración Pública*, 217, 2022, p. 172, doi: <https://doi.org/10.18042/cepc/rap.217.05>; y LÓPEZ TUR, T., «Producto defectuoso...», cit., p. 57. JORQUI AZOFRA, M., *Responsabilidad civil...*,

En cualquier caso, la citada sentencia prosigue afirmando que los Derechos nacionales pueden establecer por otra vía la responsabilidad del prestador de servicios por daños causados por el uso de un producto defectuoso, siempre que se reconozca tanto a la persona que sufrió los daños como al prestador de servicios la facultad de reclamar responsabilidad al productor. Esto abre la posibilidad de que el prestador del servicio, en lo que aquí interesa, sanitario, pueda responder con base en el art. 148 TRLGDCU o en el art. 32 LPACAP, a lo que me referiré después con más detalle.

3) Excepcionalmente, el proveedor del producto, quien responderá de forma subsidiaria cuando el productor no pueda ser identificado, a menos que, dentro del plazo de tres meses, indique al dañado o perjudicado la identidad del productor o de quien le hubiera suministrado o facilitado a él dicho producto, o cuando se trate de un producto importado, si el producto no indica el nombre del importador, aun cuando se indique el nombre del fabricante; o de forma directa, conforme al art. 146 TRLGDCU, cuando sea doloso, es decir, cuando haya suministrado el producto a sabiendas de la existencia del defecto (sin perjuicio de la acción de repetición contra el productor).

De acuerdo con todo lo anterior, cabe afirmar que actualmente cabe demandar por daños causados por sistemas inteligentes defectuosos (o máquinas que incorporan a los anteriores) en el ámbito sanitario, con base en el régimen especial de los arts. 135 y ss. TRLGDCU, al fabricante o importador de la máquina y del SIA (integrado o no en un robot), al prestador del servicio sanitario (si se sigue una interpretación literal del art. 5) y, excepcionalmente, al proveedor.

¿Qué novedades introduce la PDRCPD a este respecto?

Pues bien, para empezar, la categoría de «productor» desaparece y es sustituida por la «operadores económicos», que engloba a todo fabricante de un producto o componente, al proveedor de un servicio conexo, al representante autorizado, al importador, al prestador de servicios de tramitación de pedidos a distancia y al distribuidor [art. 4.14)]. El art. 8 PDRCPD se encarga de determinar cuáles de los mencionados operadores económicos son responsables de los productos defectuosos. Y lo hace, al igual que la vigente Directiva, distinguiendo entre unos responsables directos y unos subsidiarios. Así, como regla general responderán por los daños causados por productos defectuosos:

a) El fabricante de un producto defectuoso. En relación con este sujeto, la Propuesta contiene diversas previsiones dignas de mención:

1. La responsabilidad del fabricante abarcará también cualquier daño causado por un componente defectuoso cuando esté integrado en

cit., p. 204, por su parte, descarta esa interpretación literal y afirma que «habrá que seguir una interpretación que limite la remisión del art. 138 al artículo 5 sólo en lo referente al productor parte».

un producto bajo su control o esté interconectado con él (art. 8.1 *in fine*)¹¹¹.

2. Cualquier persona física o jurídica que modifique sustancialmente un producto fuera del control del fabricante y que posteriormente lo comercialice o ponga en servicio se considerará fabricante del producto (art. 8.2). A este respecto, por «modificación sustancial» se entiende «toda modificación de un producto después de su introducción en el mercado o su puesta en servicio: a) que se considera sustancial con arreglo a las normas nacionales o de la Unión aplicables en materia de seguridad de los productos; o b) cuando las normas nacionales o de la Unión aplicables a la seguridad de un producto no establezcan ningún umbral sobre lo que debe considerarse una modificación sustancial, que: i) cambie el rendimiento, la finalidad o el tipo originales del producto, sin que dicho cambio se haya previsto en la evaluación inicial de riesgos del fabricante; y ii) cambie la naturaleza del peligro, cree un nuevo peligro o aumente el nivel de riesgo» (art. 4.18)¹¹².

¹¹¹ Según el cdo. 18, los servicios conexos y otros componentes, incluidas las actualizaciones y mejoras de programas informáticos, deben también considerarse bajo el control del fabricante cuando este autorice o consienta su integración, interconexión o suministro por parte de un tercero, por ejemplo cuando el fabricante de un aparato doméstico inteligente consienta en que un tercero facilite actualizaciones de programas para el aparato del fabricante o cuando un fabricante presente un servicio o componente conexos como parte del producto aunque sea suministrado por un tercero. Ahora bien, no debe considerarse que un fabricante haya dado su consentimiento a la integración o interconexión simplemente por prever la posibilidad técnica de la integración o interconexión, por recomendar determinadas marcas o por no prohibir posibles servicios o componentes conexos.

¹¹² En cualquier caso, esta previsión está en línea con el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo, que considera como fabricante, y, por tanto, sujeto a las obligaciones del fabricante, a quien modifique sustancialmente un producto. Aplicado a los sistemas inteligentes, ello significa que deben someterse a una evaluación de conformidad cada vez que se introduzca en ellos una modificación sustancial (JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 213). En la misma línea, el art. 43.4 RIA dispone que los sistemas de IA de alto riesgo que ya hayan sido objeto de un procedimiento de evaluación de la conformidad se someterán a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue actual; aclarando, a estos efectos, que en el caso de los sistemas de IA de alto riesgo que continúen aprendiendo tras su introducción en el mercado o su puesta en servicio, no se considerarán modificaciones sustanciales los cambios en el sistema de IA de alto riesgo y su funcionamiento que hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y figuren en la información recogida en la documentación técnica mencionada en el anexo IV, punto 2, letra f).

Como apunta LÓPEZ TUR, en el ámbito sanitario esta previsión podría implicar que los centros sanitarios sustituyeran al fabricante como responsable de los daños causados al paciente¹¹³.

b) El fabricante de un componente defectuoso, cuando esté integrado en un producto bajo su control o esté interconectado con él y lo haya causado, y sin perjuicio de la responsabilidad del fabricante a que se refiere la letra a).

A estos efectos, entre los componentes de un producto se encuentran las actualizaciones y mejoras de los productos digitales, incluidos los SIA, con independencia de que sean bienes o se realicen en régimen de prestación de servicios¹¹⁴. De manera que la víctima que sufre daños por actualizaciones y mejoras de un sistema inteligente puede ir contra el fabricante de las actualizaciones y/o mejoras y contra el fabricante del sistema en el que se integran cuando dicha integración se haya producido bajo su control¹¹⁵.

c) En el caso de un fabricante de un producto o componente establecido fuera de la Unión, y sin perjuicio de la responsabilidad de dicho fabricante: i) el importador de un producto o componente defectuoso; ii) el representante autorizado del fabricante; y iii) cuando no haya un importador establecido en la Unión o un representante autorizado, el prestador de servicios de tramitación de pedidos a distancia.

Excepcionalmente, cuando ninguno de los sujetos anteriores pueda ser identificado, los EEMM deberán garantizar que responda cada distribuidor del producto defectuoso siempre que la persona perjudicada haya solicitado al distribuidor que identifique a un operador económico de entre los mencionados en el apartado 1 y establecido en la Unión, o a su propio distribuidor que le haya suministrado el producto y dicho distribuidor no identifique a un operador económico o a su propio distribuidor, en el plazo de un mes a partir de la recepción de la solicitud (art. 8.4). La misma norma se aplicará a cualquier proveedor de una plataforma en línea que permita a los consumidores celebrar contratos a distancia con comerciantes y que no sea un operador económico, siempre que se cumplan las condiciones del art. 6.3 Reglamento (UE) 2022/2065.

En el texto aprobado el 12 de marzo de 2024 por el PE en primera lectura, se añade que cuando las víctimas no obtengan una indemnización porque ninguna de las personas mencionadas pueda ser considerada responsable en virtud

¹¹³ LÓPEZ TUR, T., «Inteligencia artificial y responsabilidad civil en el ámbito sanitario», en *Derecho y salud: retos jurídicos actuales*, dir. por López Sánchez, C. y Ortiz Fernández, M., Aranzadi, Cizur Menor (Navarra), 2023, p. 264.

¹¹⁴ ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 149.

¹¹⁵ HERBOSA MARTÍNEZ, I., «Encaje de...», cit., pp. 84 y ss.

de la Propuesta o porque sean insolventes o hayan dejado de existir, los EEMM pueden utilizar los sistemas nacionales de indemnización sectoriales en vigor o establecer otros nuevos con arreglo al Derecho nacional, que, preferiblemente, no se financiarán con ingresos públicos, para indemnizar adecuadamente a las personas que hayan sufrido daños causados por productos defectuosos.

Para finalizar este apartado, cabe recordar que, conforme al art. 76 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (en adelante, LCS), el asegurador de cualquiera de los sujetos responsables según el régimen específico para daños causados por productos defectuosos puede ser demandado¹¹⁶.

3.2.2. Concurrencia de sujetos responsables

De acuerdo con la normativa vigente, puede haber más de un sujeto que deba responder por el daño causado por un producto defectuoso. Pensemos, por ejemplo, en los daños causados a un paciente por los fallos cometidos por un robot quirúrgico debidos a un defecto de diseño conocido por el proveedor del producto. En tales casos, el art. 132 TRLGDCU, de conformidad con el art. 5 Dir. 85/374/CEE, impone la responsabilidad solidaria frente al perjudicado de todas las personas responsables del mismo daño por aplicación del Libro Tercero; sin perjuicio de la acción de repetición que corresponde al que hubiera respondido ante el perjudicado frente a los otros responsables, según su participación en la causación del daño.

En la misma línea, el art. 12 PDRDPD dispone que «sin perjuicio de las disposiciones nacionales en relación con el derecho de repetición, los EEMM garantizarán que, cuando dos o más operadores económicos sean responsables de los mismos daños con arreglo a la presente Directiva, puedan ser considerados responsables conjunta y solidariamente».

Se ha de valorar positivamente la referencia a la acción de regreso, incorporada por el PE en el texto aprobado en marzo de 2024; aunque, como apuntan ciertos autores, sería deseable que el texto definitivo regulase cómo deben ser esas acciones de regreso, dadas las diferencias imperantes en su configuración en los distintos Estados miembros¹¹⁷.

Ahora bien, como novedad destacable, tras su modificación por el PE de marzo de 2024, el art. 13 de la Propuesta deniega la acción de repetición al fabricante que incorpore un componente de un programa informático defec-

¹¹⁶ Ver, en relación con los medicamentos y productos sanitarios, ÁLVAREZ OLALLA, P., «Daños causados...», cit., pp. 3377-3380.

¹¹⁷ MARTÍN CASALS, M., «Desarrollo tecnológico...», cit., p. 135; ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 27, y «La responsabilidad civil...», cit., p. 387.

tuoso que cause daños en dos supuestos: a) cuando el fabricante del componente de programa informático defectuoso, en el momento de la introducción en el mercado de ese componente de programa informático, era una microempresa o una pequeña empresa¹¹⁸; y b) cuando el fabricante que incorporó el componente de programa informático defectuoso en el producto acordó contractualmente con el fabricante del componente de programa informático defectuoso renunciar a ese derecho. Esta renuncia por vía contractual, no obstante, debe entenderse posible con carácter general, y, de hecho, en relación con la legislación vigente, se suele destacar que el régimen de las acciones de repetición varía, en la práctica, en función de las relaciones comerciales o de colaboración empresarial existentes entre todos los sujetos que intervienen en la distribución y comercialización de los productos y la prestación de servicios¹¹⁹.

Por otro lado, el vigente art. 133 TRLGDCU (procedente del art. 8.1 Dir. 85/374/CE) establece que la responsabilidad prevista en el Libro Tercero no se reducirá cuando el daño sea causado conjuntamente por un defecto del bien o servicio y por la intervención de un tercero; como podría ser el caso de los daños sufridos por un neonato como consecuencia de una cesárea tardía debida a que, por los errores cometidos en la organización de turnos por una herramienta de gestión hospitalaria (debidos tanto a un defecto del sistema como a un uso incorrecto por parte del centro sanitario), se atendió de forma tardía a la madre. No obstante -prosigue el precepto-, el sujeto responsable que hubiera satisfecho la indemnización podrá reclamar al tercero la parte que corresponda a su intervención en la producción del daño.

La PDRDPD va más allá en su última versión aprobada por el PE en marzo de 2024, al disponer, en su art. 13.1, que «[s]in perjuicio de lo que indique el Derecho nacional en cuanto al derecho de repetición, los Estados miembros garantizarán que la responsabilidad de un operador económico no se reduzca o anule cuando los daños sean causados tanto por el carácter defectuoso de un producto como por un acto u omisión de un tercero». El PE ha añadido las palabras «o anule», con la intención de que el operador económico demandado no pueda quedar exonerado de responsabilidad aun cuando pueda demostrar que el daño fue exclusivamente causado por

¹¹⁸ Por tales se entiende «una empresa que, evaluada junto con todas sus empresas asociadas en el sentido del artículo 3, apartado 2, del anexo de la Recomendación 2003/361/CE, en su caso, sea una microempresa tal como se define en el artículo 3, apartado 3, de ese anexo si alguna de ellas es una microempresa, tal como se define en el artículo 2, apartado 3, del anexo, o una pequeña empresa, tal y como se define en el artículo 2, apartado 2, del anexo».

¹¹⁹ PARRA LUCÁN, M.^a Á., *La protección del consumidor frente a los daños. Responsabilidad civil del fabricante y del prestador de servicios*, Reus, Madrid, 2011, p. 173; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 239.

un tercero; aunque, de ser esto así, como creo que es, debería modificarse también el resto del precepto para que rezase «cuando los daños sean causados tanto por el carácter defectuoso de un producto como por un acto u omisión de un tercero *o por el acto u omisión exclusivos de un tercero*» (el subrayado es mío). Con esta previsión, el PE insiste en la configuración de la responsabilidad del operador económico como una «garantía» frente a las víctimas -de tal manera que, con independencia de las pertinentes acciones de regreso frente al tercero, los operadores siempre deberían pagar la indemnización íntegra al perjudicado-, como ya hiciera en su Propuesta de Reglamento de 2020¹²⁰.

Por lo que se refiere a la intervención de la víctima o de una persona de la que aquella sea responsable en la causación del daño, tanto el art. 8.2 Dir. 85/374/CE (incorporado en el art. 145 TRLGDCU) como el art. 13.2 PDRDPD prevén conforme a las reglas generales, que la responsabilidad del operador económico pueda reducirse o anularse «cuando el daño sea causado conjuntamente por un defecto del producto y por culpa de la persona perjudicada o de una persona de la que la persona perjudicada sea responsable» (texto de la Propuesta). En este caso, entiendo que la redacción debería ser modificada en dos puntos: en primer lugar, sería más correcto hacer referencia a la conducta de la víctima o de las personas cuyos actos originan su responsabilidad por hecho ajeno, porque, en realidad, es esta conducta, y no la negligencia, la que interrumpe el nexo de causalidad, aunque esta sea la terminología tradicional en responsabilidad civil¹²¹; y en segundo lugar, igual que en el caso de la intervención de un tercero, sería más exacto añadir una referencia a la intervención exclusiva (y no solo a la concurrente) del perjudicado o de una persona de la que este sea responsable.

En cualquier caso, a nuestros efectos, la norma implica que si, por ejemplo, un usuario-paciente omite absolutamente las instrucciones de uso de un SIA, conociéndolas de antemano por haber sido informado (tanto de su funcionalidad como de sus riesgos), no podrá reclamar resarcimiento alguno por el daño que el sistema pueda irrogar exclusivamente por esa razón¹²².

¹²⁰ Así lo pone de relieve también ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 28. Esta autora recuerda, asimismo, que el EUROPEAN LAW INSTITUTE (ELI) *Draft of a Revised Product Liability Directive*, 2022, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf, p. 32, también parece apuntar esa posibilidad cuando en su propuesta de régimen de responsabilidad de productos defectuosos señala que la responsabilidad de un operador económico no debería quedar «excluida» ni reducida cuando el hecho de un tercero interfiera en la causación del daño.

¹²¹ Así lo subraya también ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 28.

¹²² El ejemplo es de LUQUIN BERGARECHE, R., «Responsabilidad contractual...», cit., p. 331.

3.3. SUJETOS LEGITIMADOS PARA EJERCITAR ACCIONES POR DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS

El art. 128 TRLGDCU reconoce a «todo perjudicado» el derecho a ser indemnizado, de acuerdo con el régimen recogido en el Libro Tercero de dicho texto legal («Responsabilidad civil por bienes o servicios defectuosos»), por los daños causados por productos o servicios defectuosos. Esta previsión procede de la derogada Ley 22/1994 de incorporación a nuestro ordenamiento jurídico de la Directiva de 1985, si bien el citado art. 128 TRLGDCU la ha extendido, como vemos, a los servicios defectuosos, lo cual es discutible, como después se verá.

En cualquier caso, centrándonos ahora en los daños causados por productos defectuosos, interesa destacar que el de «perjudicado» es un concepto más amplio que el de consumidor y usuario, que comprende a cualquier persona (física o jurídica) o entidad sin personalidad jurídica sea o no consumidora y que es el que debe manejarse en relación con la responsabilidad por daños causados por productos defectuosos. Así lo dispone el art. 3 TRLGDCU, cuando, tras establecer que, a los efectos de la aplicación de dicho texto legal, son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión, así como las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial, añade que eso es así «sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto», que se refieren, respectivamente, a la responsabilidad civil por daños derivados de bienes o servicios y a los viajes combinados y servicios de viaje vinculados.

No obstante, esta categoría tan amplia de «perjudicado» se ve restringida por la delimitación de los daños indemnizables a través de este régimen, ya que deben tratarse de daños causados por muerte o lesiones corporales o daños causados a una cosa (incluida su destrucción) que no sea el propio producto defectuoso, a condición de que tal cosa sea de las que objetivamente se destinan al uso o consumo privados y a tal fin la haya utilizado principalmente el perjudicado (art. 9 Dir. 85/374/CEE y art. 129 TRLGDCU). Por tanto, quedan fuera de la legitimación activa para ejercitar la acción indemnizatoria con base en el régimen especial de responsabilidad civil por daños causados por productos defectuosos las personas jurídicas con ánimo de lucro y las que no lo tengan (como los hospitales o centros de salud públicos) pero utilicen el producto en el ámbito de una actividad empresarial, ya que en ningún caso podrá darse el requisito de que la cosa dañada sea de las que se destinan a uso o consumo privado y en tal concepto haya sido usada por el perjudicado.

La PDRDPD, por su parte, restringe el abanico de perjudicados, limitándolo a las personas físicas (art. 5). Se excluye así, a las personas jurídicas sin ánimo de lucro y las entidades sin personalidad jurídica de la posibilidad de lograr una indemnización por esta vía, lo cual ha sido criticado, a mi juicio con razón, puesto que implicará un retroceso respecto de la legislación vigente¹²³.

En cualquier caso, en lo que aquí interesa, ni de acuerdo con la normativa vigente ni con la que vendrá, los profesionales sanitarios, hospitales y centros de salud pueden reclamar una indemnización al responsable de los daños causados por un sistema inteligente defectuoso¹²⁴.

En otro orden de cosas, el apdo. 2 del art. 5 PDRDPD permite que las reclamaciones de indemnización puedan ser presentadas, no solo por la persona física perjudicada, sino también por una persona que: a) sea sucesora o se haya subrogado en el derecho de aquella en virtud del Derecho de la Unión o nacional o de un contrato (p. ej., los herederos de la víctima fallecida)¹²⁵; o b) actúe en nombre de una o varias personas perjudicadas de acuerdo con el Derecho de la Unión o nacional.

3.4. FUNDAMENTO DE LA RESPONSABILIDAD Y CAUSAS DE EXONERACIÓN

El régimen de responsabilidad que la Directiva 85/374/CEE instaaura para los daños causados por productos defectuosos es de carácter objetivo, de manera que no es precisa la culpa o negligencia del agente para que nazca su responsabilidad. Así se desprende, en efecto, tanto del art. 1 (transpuesto en el art. 135 TRLGCU), en virtud del cual «[e]l productor será responsable de los daños causados por los defectos de sus productos» como del art. 4 (incorporado en el art. 139 TRLGDCU), que establece que «[e]l perjudicado deberá probar el daño, el defecto y la relación causal entre el defecto y el daño».

No hay cambios a este respecto en la PDRDPD. Sí los hay, por el contrario, en las causas de exoneración de responsabilidad, algunas de las cuales, por

¹²³ GÓMEZ LIGÜERRE, C., «La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos», *Indret* 4.2022, Editorial; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., pp. 141-142; LÓPEZ TUR, T., «Producto defectuoso...», cit., pp. 54-55. Por otro lado, el razonamiento expuesto en el cdo. 22 es un tanto extraño: «En consonancia con el objetivo de la presente Directiva de poner la indemnización únicamente a disposición de las personas físicas, los daños a bienes utilizados exclusivamente con fines profesionales no deben ser indemnizados en virtud de la presente Directiva». ¿Acaso no existe el empresario persona física?

¹²⁴ En el mismo sentido, ÁLVAREZ OLALLA, P., «Daños causados...», cit., p. 3381.

¹²⁵ En relación con ello, el cdo. 27 dispone que «[e]n la medida en que el Derecho nacional lo prevea, el derecho a indemnización de los perjudicados debe aplicarse tanto a las víctimas directas que sufran daños directamente causados por un producto defectuoso como a las víctimas indirectas que sufran perjuicio como consecuencia de los daños sufridos por la víctima directa».

cierto, como la de los riesgos del desarrollo, introducen un matiz subjetivo en la responsabilidad, que trata de ser corregido por el TJUE en su interpretación de la norma, como después se verá.

Así, la PDRDPD mantiene las causas de exoneración recogidas en la Directiva vigente, aunque adaptándolas a los propósitos de la nueva regulación, y añade algunas nuevas. En efecto, de acuerdo con el art. 10.1 de la Propuesta, los operadores económicos a que se refiere el artículo 8 no serán responsables de los daños causados por un producto defectuoso si demuestran:

- 1) En el caso de un fabricante o importador, que no ha introducido el producto en el mercado ni lo ha puesto en servicio; o, en el caso de un distribuidor, que no ha comercializado el producto [letras a) y b)]. Según se desprende del cdo. 49 de la Propuesta, la exoneración se justifica, en estos supuestos, porque los mencionados sujetos no deben ser responsables cuando puedan demostrar que una persona distinta de ellos ha provocado la salida del producto del proceso de fabricación en contra de su voluntad.
- 2) Que es probable que el defecto que causó el daño no existiera en el momento en que el producto fue introducido en el mercado, puesto en servicio o, en el caso de un distribuidor, comercializado, o que este defecto se produjo después de ese momento [letra c)]. Ahora bien, el operador económico no podrá hacer uso de esta causa de exoneración, según el art. 10.2 de la Propuesta, «cuando el defecto de un producto se deba a alguna de las causas siguientes, siempre que esté bajo el control del fabricante: a) un servicio conexo; b) programas informáticos, incluidas las actualizaciones o mejoras de programas informáticos; c) una falta de actualizaciones o mejoras de los programas informáticos necesarias para mantener la seguridad; d) una modificación sustancial del producto». Hay que entender, por tanto, que el operador económico sí quedará exonerado cuando los servicios conexos, los programas informáticos, las actualizaciones o mejoras y las modificaciones sustanciales no estén bajo su control, como, por ejemplo, si el propietario de un sistema inteligente no instala una actualización que debería (cdo. 51).
- 3) Que el defecto se debe a que el producto se ajusta a los requisitos legales [letra d)].
- 4) Que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso [letra e)]. Esta exoneración de responsabilidad con base en los deno-

minados «riesgos del desarrollo» o «riesgos del progreso» ya está prevista en la Directiva vigente, aunque con libertad de los EEMM para excluirla; de hecho, de acuerdo con el vigente art. 140.1.e) TRLGDCU, esta causa de exoneración no es aplicable en el caso de medicamentos, alimentos o productos alimentarios destinados al consumo humano, pero nada se dice sobre los productos sanitarios¹²⁶.

En cualquier caso, la exoneración por esta causa -que, *de facto*, implica la introducción de la culpa o negligencia como criterio de imputación de la responsabilidad, lo cual ha sido criticado por la doctrina¹²⁷-, puede dar mucho juego en la responsabilidad por daños causados por SIA defectuosos, cosa que no convence a todos¹²⁸; aunque se encuentran voces que defienden que la oponibilidad de esta cláusula favorece el progreso de la ciencia y la técnica, en la medida en que su eliminación desalentaría la inversión en nuevas tecnologías, máxime si se tiene en cuenta que, con la rapidez que avanzan los cambios en la ciencia y en la técnica, en cuestión de breves períodos de tiempo, los defectos que no puedan ser apreciados pasen a ser fácilmente descubiertos y eliminados¹²⁹ [letra e)].

- 5) En el caso de un fabricante de un componente defectuoso, que el carácter defectuoso del producto a que se ha incorporado el componente sea imputable al diseño del producto o a las instrucciones da-

¹²⁶ Si bien ciertos autores sostienen que la misma razón jurídica concurre para incluir a los productos sanitarios en la exclusión de la mencionada cláusula de exoneración, especialmente los clasificados con nivel IIa, IIb y III, que son productos destinados a introducirse en el cuerpo humano, estén o no destinados a permanecer en él (en este sentido, PARRA LUCÁN, M.^a Á., *La protección...*, cit., p. 184; GIL SALDAÑA, M., *El producto sanitario defectuoso en Derecho español*, Atelier, Barcelona, 2008, p. 180; y ÁLVAREZ OLALLA, P., «Daños causados...», cit., p. 3374).

¹²⁷ BERCOVITZ RODRÍGUEZ-CANO, R., «La responsabilidad de los fabricantes en la Directiva de las Comunidades Europeas de 25 de junio de 1985», *Estudios sobre consumo*, núm. 7, 1986, p. 7; ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., pp. 43-44.

¹²⁸ En contra de su aplicación a los SIA, NÚÑEZ ZORRILLA, M.^a C., *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019, p. 41; MONJE BALMASEDA, Ó., «Robótica y...», cit., p. 452, para quien solo en los casos de fuerza mayor, esto es, en situaciones en las que el evento dañoso proceda de riesgos externos y, por tanto, ajenos al círculo de actividad del sistema, debemos admitir una exoneración de responsabilidad. DÍAZ ALABART, S., *Robots y...*, cit., p. 113, por su parte, estima que, de mantenerse esta causa de exoneración para los robots, debería al menos establecerse una excepción para los que interactúen con personas vulnerables y los que tengan contacto físico con las personas.

¹²⁹ Defienden esta opinión, entre otros, GÓMEZ LIGÜERRE, C. y GARCÍA MICÓ, T. G. «Liability for...», cit., p. 509, y ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 45. En contra, respecto de los vehículos autónomos, NAVARRO-MICHEL, M., «Vehículos automatizados y responsabilidad por producto defectuoso», *Revista de Derecho Civil*, vol. VII, núm. 5 (octubre-diciembre, 2020), pp. 215-216, señala que la eliminación de esta cláusula llevaría consigo el aumento de la confianza de la sociedad en el sector de la tecnología, lo que revertiría en que se adquirirían más productos tecnológicos nuevos porque los ciudadanos entenderían que los que hay en el mercado siempre son seguros; aparte de que, al final, garantizar la seguridad implica también para los fabricantes reducir los costes por indemnizaciones.

- das por el fabricante del producto al fabricante de dicho componente [letra f)]. Esta excepción, que también existe en la Dir. 85/374/CEE, permitirá al fabricante del *software* de un robot, por ejemplo, cuando el fabricante del *hardware* sea otro, liberarse de responsabilidad¹³⁰.
- 6) En el caso de una persona que modifica un producto según lo dispuesto en el artículo 8, apartado 2, que el carácter defectuoso que haya causado el daño esté relacionado con una parte del producto no afectada por la modificación [letra g)]. Esta causa de exoneración, introducida *ex novo* por la Propuesta, se explica, en términos de causalidad jurídica, por el hecho de que la modificación no ha incrementado el riesgo de producción de daños, de modo que estos no pueden imputarse objetivamente a dicha modificación¹³¹.

4. RÉGIMEN DE RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR SERVICIOS SANITARIOS DEL ART. 148 TRLGDCU¹³²

4.1. ÁMBITO DE APLICACIÓN Y FUNDAMENTO DE LA RESPONSABILIDAD

El art. 148 TRLGDCU establece un régimen especial de responsabilidad civil -respecto del general regulado en el art. 147 del mismo texto legal- para los servicios sanitarios, entre otros. Según el apartado primero del citado precepto, «[s]e responderá de los daños originados en el correcto uso de los servicios, cuando por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario». A ello añade el apartado segundo que «[e]n todo caso, se consideran sometidos a este régimen de responsabilidad los servicios sanitarios, los de reparación y mantenimiento de electrodomésticos, ascensores y vehículos de motor, servicios de rehabilitación y reparación de viviendas, servicios de revisión, instalación o similares de gas y electricidad y los relativos a medios de transporte». Finalmente, el apartado tercero establece un límite para las responsabilidades derivadas de este artícu-

¹³⁰ Así lo pone de relieve, asimismo, MONTERROSO CASADO, E., «Responsabilidad civil...», cit., p. 116.

¹³¹ ATIENZA NAVARRO, M.^a L., «¿Una nueva...», cit., p. 47.

¹³² Realizo un estudio detallado sobre este precepto en EVANGELIO LLORCA, R., «A vueltas con la responsabilidad por daños derivados de servicios sanitarios al amparo del artículo 148 TRLGDCU», en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en homenaje al Profesor Dr. Roca Guillamón*, Aranzadi, Cizur Menor (Navarra), 2021, pp. 475-532.

lo de 3.005.060,52 euros, sin perjuicio de lo establecido en otras disposiciones legales.

Pues bien, la redacción del precepto, junto con el hecho de que el art. 147 TRLGDCU disponga, como regla general, en materia de daños causados por servicios, una responsabilidad civil subjetiva con inversión de la carga de la prueba de la culpa, sugiere que la especialidad del art. 148 TRLGDCU -que procede del derogado art. 28 LGDCU- consiste en el establecimiento de una responsabilidad civil objetiva para determinados servicios, entre ellos, los sanitarios.

A estos efectos, la expresión «servicios sanitarios» se interpreta de forma restrictiva por el TS, entendiendo que se circunscribe a los aspectos funcionales de dicho servicio, es decir, a los aspectos organizativos o de prestación de los servicios sanitarios, sin alcanzar a los daños imputables directamente a los actos médicos¹³³ (esto es, a la actividad médica de los profesionales sanitarios)¹³⁴. En lo que ahora interesa, se incluirían aquí, por ejemplo, los daños por uso de sistemas inteligentes de triaje en los servicios de urgencias o de herramientas de IA utilizadas en la planificación de los turnos en los servicios de hospitales, así como daños derivados de un incorrecto almacenamiento de los productos o de no proceder a las revisiones previstas por el fabricante.

Esta interpretación del Alto Tribunal encuentra su explicación, sin duda, en el hecho de que incluir la actuación médica implicaría tirar por tierra la tesis pacífica, tanto en la doctrina como en la jurisprudencia, de que la acti-

¹³³ El art. 6.1 del Código de Deontología Médica 2022 define el «acto médico» «toda actividad lícita y guiada por la *lex artis ad hoc* desarrollada por un profesional médico legítimamente capacitado, ya sea en su ámbito asistencial, docente, investigador, pericial, de actividad evaluadora, inspectora, de planificación, gestión sanitaria u otros. Se incluyen actos diagnósticos, terapéuticos o de alivio del sufrimiento, así como de la preservación, promoción y prevención de la salud, por medios directos e indirectos».

¹³⁴ Ver, entre muchas otras, las sentencias del TS de: 26 marzo 2004 (RJ 1668); 7 mayo 2007 (RJ 3553); 15 noviembre 2007 (RJ 8110); 28 noviembre 2007 (RJ 8427); 943/2008 23 octubre 2008 (RJ 5789); 4 junio 2009 (RJ 3380); 27 septiembre 2010 (RJ 7141); 20 mayo 2011 (RJ 3982); STS 16 enero 2012 (RJ 1748); STS 18 mayo 2012 (RJ 6356); 3 julio 2013 (RJ 4380); 20 julio 2009 (RJ 3161); 18 julio 2019 (RJ 3471).

Debe advertirse que también hay resoluciones que han aplicado el derogado art. 28 LGDCU (junto con el Código Civil) para responsabilizar al empresario principal por daños causados por la actuación médica de un dependiente [SSTS 30 diciembre 1999 (RJ 9496), 30 diciembre 1999 (RJ 4974), 19 junio 2001 (RJ 4974), 18 diciembre 2002 (RJ 47)], e incluso al facultativo que en ocasiones es, además, el único demandado [en este sentido, SSTS 29 noviembre 2002 (RJ 10404) y 31 enero 2003 (RJ 4974), si bien en esta última hubo un voto particular del Magistrado F. Marín Castán en contra de la aplicación del art. 28 LGDCU a la prestación médica, en la medida en que «la jurisprudencia, entendida como criterio constante y reiterado en la decisión de casos semejantes, rechaza abiertamente la responsabilidad objetiva del médico o del cirujano»; y aunque no de forma tan clara, 15 septiembre 2003 (RJ 6418), 18 marzo 2004 (RJ 1823) y 16 abril 2007 (RJ 4332)].

vidad desplegada por médicos y demás profesionales sanitarios es en general una obligación de medios, que debe medirse en términos de diligencia y a la que, por tanto, no se debe aplicar un régimen de responsabilidad objetiva¹³⁵. En este sentido, se declara que la aplicación del régimen especial de responsabilidad objetiva a la actividad médica conduciría a «una consecuencia en sí misma tan indeseable e injustificable, incluso en el plano puramente teórico, de acabar midiendo por el mismo rasero al médico diligente que al negligente, al cuidadoso que al descuidado, en cuanto ambos responderían siempre y por igual de cualquier resultado no deseado de su intervención»¹³⁶.

También la doctrina mayoritaria sostiene que la responsabilidad objetiva del art. 148 TRLGDCU no debe ser aplicada a la responsabilidad personal del profesional sanitario sino solamente al funcionamiento del servicio¹³⁷.

A mi juicio, no se puede negar que la actuación médica forma parte de la prestación de un servicio sanitario (la más importante, además), por lo que habría que concluir que está sujeta al art. 148 TRLGDCU. Ahora bien, la consecuencia que de ello se deriva, esto es, la aplicación de un régimen de responsabilidad objetiva a la actividad médica, es contraria a los principios más que asentados en esta materia, según los cuales es inherente a los actos médicos propiamente dichos la aplicación de criterios de responsabilidad fundados en la negligencia por incumplimiento de la *lex artis ad hoc*, como reitera el TS. Ello implicaría, además, un diferente tratamiento jurídico a realidades sustancialmente idénticas, pues se valorarían de diferente manera las responsa-

¹³⁵ Así se entiende por el TS en la actualidad incluso en el ámbito de la medicina satisfactiva: la obligación del médico -se afirma- es obligación de medios y no de resultado, salvo que el resultado se pacte o se garantice [por todas, STS 27 septiembre 2010 (RJ 7141)].

¹³⁶ STS 28 noviembre 2007 (RJ 8427), siguiendo el voto particular de Marín Castán en la citada STS 31 enero 2003.

¹³⁷ GALÁN CORTÉS, J., *Responsabilidad civil...*, cit., p. 289; ASÚA GONZÁLEZ, C. I., «Responsabilidad sin culpa en la medicina privada: el artículo 28 LGDCU», en Moreno Martínez, J. A. (coordinador), *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007, p. 59, y «Responsabilidad civil médica», en *Tratado de Responsabilidad Civil*, coord., por L. F. Reglero Campos y J. M. Busto Lago, vol. II, 5ª. ed., Thomson Reuters-Aranzadi, 2014, p. 1102; LUNA YERGA, Á., «Olvido de una gasa durante una intervención quirúrgica. Comentario a la STS, 1ª, 29.11.2002», *InDret*, 2-2003, p. 11; RUIZ JIMÉNEZ, J., «La aplicación de responsabilidad objetiva en los servicios sanitarios», *RCDI*, núm. 700, marzo-abril 2007, p. 851; PARRA LUCÁN, M.ª Á., *La protección...*, cit., pp. 261-262, y «Responsabilidad civil...», cit., p. 2108; CUETO PÉREZ, M., «Jurisprudencia en...», cit., p. 173.

En contra, consideran que la responsabilidad médica propiamente dicha debe entenderse incluida también en el art. 28 LGDCU y el vigente art. 148 TRLGDCU: BERCOVITZ RODRÍGUEZ-CANO, R., «Comentario a la STS de 1 de julio de 1997», *CCJC*, núm. 45, 1997, p. 1219; GÓMEZ CALLE, E., «El fundamento de la responsabilidad civil en el ámbito médico-sanitario», *ADC*, vol. 51, núm. 4, 1998, p. 1755; PEÑA LÓPEZ, F., «Comentario a la STS 11 febrero 1998», *CCJC*, núm. 47, 1998, pp. 782 y 787; y PANIZA FULLANA, A., «La responsabilidad civil médico-sanitaria y la LGDCU», *Revista Doctrinal Aranzadi Civil-Mercantil*, 1998, pp. 14-16.

bilidades de facultativos y personal sanitario de la medicina privada y pública (ya que la responsabilidad civil de estos últimos profesionales sólo puede ser exigida, con carácter general, por la Administración Pública en vía de regreso cuando hubieran incurrido en dolo o culpa grave, lo que excluye su responsabilidad para la mayor parte de casos en que su conducta no sea constitutiva de delito); amén de conducir a un incremento de la medicina defensiva¹³⁸.

Así las cosas, comprendo y comparto, que, aunque desde un punto de vista técnico resulte más que forzado, la jurisprudencia -salvo en alguna sentencia de forma excepcional- y parte relevante de la doctrina se decanten por una interpretación restrictiva de la expresión «servicios sanitarios» en los términos apuntados.

Esto aclarado, creo que, a pesar de que en el art. 148 TRLGDCU no se exige que el servicio sea defectuoso (a diferencia de lo que ocurre en sede de responsabilidad civil por productos), la imputación objetiva del daño al prestador del servicio sanitario debe ir unida al defecto del servicio; de manera que solamente cuando el servicio sanitario sea defectuoso, se imputarán los daños al prestador. Así se desprende, además de del sentido común, de la rúbrica del Libro III: «Responsabilidad civil por bienes o servicios defectuosos»¹³⁹.

En relación con el alcance del régimen recogido en el art. 148 TRLGDCU, interesa plantear la cuestión de si el prestador del servicio sanitario responderá, con base en dicho precepto, de los daños causados por un producto defectuoso usado en la prestación del servicio. A partir de la anteriormente

¹³⁸ LUNA YERGA, Á., «Olvido de...», cit., p. 11.

¹³⁹ Como señaló CAVANILLAS MÚGICA, S., *Responsabilidad civil y protección del consumidor*, Universitat de les Illes Balears, Palma de Mallorca, 1985, p. 178, en relación con el art. 28 LGDCU.

Se unifica así, en este punto, el régimen de responsabilidad civil por bienes o servicios, en coherencia con el deber general de seguridad de productos y de servicios que el art. 11 TRLGDCU impone, deber cuyo incumplimiento seguido de la producción de un daño dará lugar a la aplicación de las reglas de responsabilidad contenidas en el citado Libro. Como subraya PASQUAU LIAÑO, M., «El defecto de seguridad como criterio de imputación de responsabilidad al empresario de servicios», en *La responsabilidad civil por daños causados por servicios defectuosos*, dir. por A. Ortí Vallejo y M.^a del C. García Garnica, 2^a ed., Thomson-Aranzadi, Navarra, 2015, p. 103, si al definir el deber positivo de seguridad la ley equipara productos y servicios, ¿por qué no equiparar el envés de una regla negativa de responsabilidad consistente, precisamente, en la infracción objetiva de aquella obligación de seguridad? PARRA LUCÁN, M.^a Á., *La protección...*, cit., pp. 257-258; y «Responsabilidad civil...», cit., p. 2103, por su parte, justifica la exigencia de que el servicio sea defectuoso en que no parece razonable imputar una responsabilidad a los prestadores de servicios por la única razón de prestar un servicio. Tal cosa -sostiene esta autora- conduciría a consecuencias poco deseables: por un lado, se reduciría de manera irrazonable la prestación de servicios cuyos riesgos la sociedad está dispuesta a soportar (parques de atracciones, deportes de riesgo), ante el temor de quienes los organizan y los prestan de verse expuestos a reclamaciones desproporcionadas; y por otro lado, se podría ver condicionado, en un modo poco beneficioso para el usuario y para la propia sociedad, el ejercicio de algunos servicios, como los médicos, con un actuar defensivo dirigido a evitar toda intervención que pudiera acarrear cierto riesgo de responsabilidad o dudas sobre la posibilidad de un éxito total.

referida STJUE de 21 diciembre 2011, en la que se afirmaba que el prestador del servicio no puede responder con base en la Directiva de productos defectuosos (pese a lo cual, como se ha visto, en España esa posibilidad resulta de la combinación de los arts. 138 y 5 del TRLGDCU), pero sí al amparo de otro régimen, la respuesta a la cuestión planteada debe ser afirmativa. En efecto, a lo que entiendo, el mero uso de un producto defectuoso en la prestación del servicio sanitario es suficiente para considerar tal servicio como defectuoso, a efectos de invocar el citado precepto; ya que quien se somete a una intervención médica u hospitalaria puede legítimamente esperar que el material, utensilios, etc. empleados son lo suficientemente seguros como para evitar riesgos añadidos a los derivados típicamente del tratamiento o la intervención¹⁴⁰. En este caso, por tanto, habrá responsabilidad solidaria del productor y del prestador del servicio por aplicación del art. 132 TRLGDCU, sin perjuicio de la acción de regreso del prestador del servicio que haya indemnizado al perjudicado frente al productor del bien defectuoso¹⁴¹.

En España, la Sala Primera del TS no cuestiona la legitimación pasiva del prestador del servicio sanitario, ni cuando es demandado junto con el fabricante¹⁴², ni cuando, como sucede más a menudo¹⁴³, se le demanda a él exclusiva

¹⁴⁰ Coincido en este punto con SANTOS MORÓN, M.^a J., «La imputación de responsabilidad médica con base en las normas de protección de consumidores: el artículo 148 TRLC», *ADC*, tomo LXX, 2017, fasc. 1, p. 148; ASÚA GONZÁLEZ, C. I., «Responsabilidad civil...», cit., p. 423; PARRA LUCÁN, M.^a Á., *La protección...*, cit., p. 285; ÁLVAREZ OLALLA, P., «Daños causados...», cit., p. 3402. Por el contrario, GÓMEZ LIGÜERRE, C., «Responsabilidad del...», cit., p. 78, estima que la regla del art. 148 TRLGDCU solamente opera en los casos en que el daño es atribuible exclusivamente al prestador del servicio, por lo que no puede fundamentar su condena cuando el daño lo ha causado el defecto del producto empleado en la prestación correcta del servicio.

¹⁴¹ En relación con ello, cabe mencionar la STS 15 noviembre 2004 (RJ 7233), que traía causa de un procedimiento anterior en el que una mutualidad había sido condenada a indemnizar a una de sus mutualistas que había contraído una hepatitis C con ocasión de una operación quirúrgica a la que había sido sometida en un centro médico de la citada entidad y en la que se le había transfundido sangre infectada. Pagada la indemnización que se acordó de forma transaccional tras la condena, la Mutualidad demandó al banco de sangre proveedor exclusivo de hemoderivados y plasma, el cual fue condenado.

¹⁴² Como ocurrió en la STS 24 septiembre 1999 (RJ 7272), en relación con un DIU defectuoso implantado en un centro público de planificación familiar, en la STS 22 noviembre 1999 (RJ 8618), sobre catéter que se rompió y quedó parcialmente dentro del cuerpo de una paciente que había sido intervenida quirúrgicamente, o la STS 4 diciembre 2007 (RJ 251) sobre contagio de hepatitis C por transfusión de sangre contaminada. Conviene recordar, a estos efectos, que la sangre y los hemoderivados deben considerarse productos defectuosos a efectos del TRLGDCU. En este sentido, el art. 140.3 se refiere a «medicamentos, alimentos o productos alimentarios destinados al consumo humano», y el art. 46 RD legislativo 1/2015, de 24 de julio, por el que se aprueba el TR de la Ley de garantías y uso racional de los medicamentos y productos sanitarios (antes, art. 40 Ley 25/1990, de 20 de diciembre, del medicamento) califican como medicamentos de origen humano «[l]os derivados de la sangre, del plasma y el resto de sustancias de origen humano (fluidos, glándulas, excreciones, secreciones, tejidos y cualesquiera otras sustancias), así como sus correspondientes derivados».

¹⁴³ Como subraya PARRA LUCÁN, M.^a Á., «Responsabilidad civil...», cit., p. 2089, es al prestador del servicio a quien, por regla general, la víctima prefiere demandar, como es lógico por la mayor facili-

o conjuntamente con los facultativos, pero no también al fabricante¹⁴⁴. Ahora bien, como regla general se excluye la responsabilidad del centro sanitario; en este sentido, tanto la STS 15 febrero 2017¹⁴⁵ como la STS 28 junio 2021¹⁴⁶ exoneraron de responsabilidad a sendas clínicas privadas por los daños derivados de la implantación de unas prótesis mamarias defectuosas que, en el momento del implante, se encontraban debidamente autorizadas por la AEMPS¹⁴⁷.

En el caso de que el prestador del servicio sanitario sea público, surgen discrepancias entre la doctrina y la jurisprudencia sobre si queda sometido al régimen del art. 148 TRLGDCU, como a continuación se verá. Por ello, analizaré esta cuestión más adelante, al referirme a la responsabilidad patrimonial de la Administración sanitaria.

4.2. SUJETO RESPONSABLE

Por lo que se refiere al sujeto responsable del daño causado por un servicio sanitario, aunque el art. 148 TRLGDCU (ni el derogado art. 28 LGDCU) no lo establezca expresamente, cabe entender que es el prestador del servicio; del que se puede asegurar, con base en el art. 2 TRLGDCU, que ha de ser un empresario, entendido este como toda persona física o jurídica que actúa en el marco de su actividad empresarial o profesional, ya sea pública o privada. Por consiguiente, según el tenor literal de la norma, pueden responder con base en el art. 148 TRLGDCU prestadores de servicios sanitarios tanto públicos como privados. La doctrina, sin embargo, suele defender que dicho régimen solamente debe aplicarse a los prestadores de servicios sanitarios privados¹⁴⁸, quedando los daños causados en centros sanitarios u hospitales públicos su-

dad en la gestión del proceso, ya que es con el prestador del servicio y no con el fabricante con quien el perjudicado tiene una relación directa, por lo que la reclamación contra él le evita tener que efectuar averiguaciones sobre todas las circunstancias relativas a proveedores sanitarios, identidad del productor, etc.

¹⁴⁴ Así ocurrió, por ejemplo, en la STS 25 enero 1997 (RJ 155), sobre medicamento defectuoso por falta de información, o la STS 17 abril 1998 (RJ 2055), sobre lesiones causadas por la rotura de una jeringa defectuosa; así como, en general, en los casos relativos a infecciones del virus VIH como consecuencia de transfusiones de sangre contaminada [entre otras, SSTS 24 junio 1997 (RJ 5208), 11 febrero 1998 (RJ 707), 26 febrero 1998 (RJ 1169), STS 28 diciembre 1998 (RJ 10161), 10 noviembre 1999 (RJ 8955), 3 diciembre 1999 (RJ 8532), 30 diciembre 1999 (RJ 9752) y 5 diciembre 2007 (RJ 469)].

¹⁴⁵ RJ 2017\583.

¹⁴⁶ RJ 2021\3016.

¹⁴⁷ Sobre la eventual responsabilidad de la AEMPS y organismos notificados, ver GRIMALT SERVERA, P., «La responsabilidad...», cit., pp. 15-19, y ÁLVAREZ OLALLA, P., «Daños causados...», cit., pp. 3396-3400.

¹⁴⁸ PARRA LUCÁN, M.^a Á., *La protección...*, cit., p. 243; SANTOS MORÓN, M.^a J., «La imputación...», cit., p. 123; PACHECO JIMÉNEZ, M.^a N., «Responsabilidad por daños desde la perspectiva del usuario de servicios sanitarios: del art. 28 LGDCU al art. 148 TRLGDCU», *Revista Jurídica sobre Consumidores y Usuarios*, núm. 4, enero 2019, p. 7 (según paginación vLex). En relación con el art. 28

jetos al régimen de la responsabilidad patrimonial de la Administración, a la que más adelante me referiré. Esta opinión no parece ser en cambio compartida por recientes sentencias de la Sala Tercera del TS sobre la responsabilidad civil de hospitales públicos por los daños causados por el uso de un gas tóxico durante intervenciones quirúrgicas, en las que se ha admitido la posible aplicación del art. 148 TRLGDCU¹⁴⁹.

Por otro lado, considero que la responsabilidad derivada del mismo solo debe atribuirse a quien asuma riesgo empresarial, y no a quien presta servicios sanitarios de forma dependiente¹⁵⁰. Por consiguiente, en los casos de servicio prestado por un profesional de la medicina (médico, enfermero, fisioterapeuta, etc.) que trabaja como asalariado en un hospital o centro sanitario o está incluido en el cuadro médico de una compañía de asistencia sanitaria, serán los principales y no el facultativo los responsables en virtud del art. 148 TRLGDCU (sin perjuicio de que se pueda exigir responsabilidad a este por la vía del art. 1902 CC). En cambio, el facultativo que ejerce la medicina como profesional autónomo o empresario individual debe quedar sometido al régimen del citado precepto¹⁵¹; incluso cuando es un profesional independiente que presta sus servicios como auxiliar en el cumplimiento de aseguradoras de servicios sanitarios (lo cual se aplicaría, asimismo, al centro sanitario)¹⁵². Ahora bien, de acuerdo con la interpretación estricta de la expresión «servicios sanitarios» que aquí se defiende, la responsabilidad del facultativo no alcanzará a la prestación médica, sino a los aspectos de funcionamiento y organización del servicio.

LGDCU, así lo destacaron también ASÚA GONZÁLEZ, C. I., «Responsabilidad sin culpa...», cit., p. 39, y LUNA YERGA, Á., «Olvido de...», cit., p. 9.

¹⁴⁹ En este sentido, SSTs (Sala de lo Contencioso) 4495/2020, ECLI:ES:TS:2020:4495; 219/2021 de 21 enero, ECLI:ES:TS:2021:219; 338/2021, de 28 enero, ECLI:ES:TS:2021:338; 2431/2021, de 9 junio, ECLI:ES:TS:2021:2431; 4317/2021, de 17 noviembre, ECLI:ES:TS:2021:4317; 4521/2021, de 1 diciembre, ECLI:ES:TS:2021:4521; 818/2022, de 23 febrero, ECLI:ES:TS:2022:818; 765/2022, de 3 marzo, ECLI:ES:TS:2022:765; 3581/2022, de 6 octubre.

Por el contrario, las SSTs de la misma Sala 5395/2010, de 13 octubre, ECLI:ES:TS:2010:5395, y 2185/2016, de 19 de mayo, ECLI:ES:TS:2016:2185, excluyeron la aplicabilidad del TRLGDCU respecto de la posible responsabilidad patrimonial de la Administración sanitaria, por entender que debía regirse por la entonces vigente Ley 30/1992.

¹⁵⁰ Son de la misma opinión ASÚA GONZÁLEZ, C. I., «Responsabilidad sin culpa...», cit., p. 61; y «Responsabilidad civil...», cit., p. 425; y PERTÍÑEZ VÍLCHEZ, F., «Daños causados por otros bienes y servicios», en *La defensa de los consumidores y usuarios*, dir. por Rebollo Puig, M. e Izquierdo Carrasco, M., Iustel, Madrid, 2011, p. 1938.

¹⁵¹ En la misma línea, ASÚA GONZÁLEZ, C. I., «Responsabilidad sin culpa...», cit., p. 39; PEÑA LÓPEZ, F., «Comentario...», cit., pp. 786-787; PARRA LUCÁN, M.^a Á., *La protección...*, cit., p. 243; SANTOS MORÓN, M.^a J., «La imputación...», cit., p. 123; ÁLVAREZ OLALLA, P., «Daños causados...», cit., pp. 3382-3383.

¹⁵² ASÚA GONZÁLEZ, C. I., «Responsabilidad sin culpa...», cit., p. 62; y «Responsabilidad civil...», cit., p. 425.

Por lo que se refiere a las compañías de asistencia sanitaria, la jurisprudencia utiliza diversos criterios, de forma alternativa o combinada, a la hora de decidir sobre su responsabilidad civil por daños. Entre tales criterios se incluye el art. 28 LGDCU, si bien la cita del mismo se hace, en la mayoría de sentencias de la Sala Primera, «como un argumento auxiliar» al resto, condición esta que ni siquiera se le reconoce en algunas sentencias, al afirmarse que los criterios de responsabilidad objetiva contemplados en el LCU únicamente son relevantes para determinar la existencia de responsabilidad por parte de los servicios médicos, sin que esta, por sí, predetermine la responsabilidad de la aseguradora. Para ello, hay que acudir al resto de criterios¹⁵³.

En cualquier caso, tal y como se ha indicado al tratar los daños causados por productos defectuosos, cuando haya varios responsables del mismo daño por aplicación de este régimen (o de cualquiera de los regulados en el Libro Tercero del TRLGDCU) lo serán solidariamente ante los perjudicados, si bien el que hubiera respondido ante estos tendrá derecho a repetir frente a los otros responsables, según su participación en la causación del daño (art. 132 TRLGDCU).

4.3. SUJETO PROTEGIDO

Como se ha señalado *supra*, en la medida en que el art. 128 TRLGDCU forma parte de las disposiciones comunes del TRLGDCU en materia de responsabilidad civil por daños causados por bienes o servicios defectuosos (Capítulo I del Título I del Libro Tercero), en principio hay que entender que es aplicable tanto a los daños procedentes de productos defectuosos como de otros bienes o de servicios. Ahora bien, según se indicó, se trata de una regla procedente de la Ley 22/1994 sobre responsabilidad civil por los daños causados por productos defectuosos, por lo que no debería alcanzar a los servicios. Por ello, en general se sostiene que el perjudicado por un servicio debe

¹⁵³ SSTs 4 diciembre 2007 (RJ 251) y 16 enero 2012 (RJ 1748). En la primera de estas sentencias, se recurrió a la naturaleza de la relación contractual entre la aseguradora y su cliente, así como al principio de apariencia y de los actos de publicidad llevados a cabo por la misma. En este sentido, el TS entendió que la obligación de la aseguradora comprendía no solamente la asunción del coste económico de las operaciones médicas, sino también su prestación por medio de médicos o establecimientos que actuaban como auxiliares contractuales para la realización de las prestaciones. De ahí se derivaba que la aseguradora «no se limitó a asumir una simple posición de aseguramiento de los costos de la asistencia, sino que su garantía se extendía contractualmente a la calidad de los servicios prestados mediante cuadros médicos objeto de una especial selección y clínicas a su servicio».

Otro criterio utilizado con frecuencia es el tipo de póliza suscrita con la entidad aseguradora, afirmándose la responsabilidad cuando se trate de un seguro de asistencia sanitaria propiamente dicho y excluyéndola cuando el contrato sea de reembolso de gastos médicos [SSTS 19 junio 2001 (RJ 4974), 27 septiembre 2010 (RJ 7141) y 24 mayo 2012 (RJ 6539)].

encajar en el concepto general de consumidor o usuario del art. 3 TRLGDCU, como se exigía respecto del art. 25 de la Ley de 1984, que concedía el derecho a ser indemnizado por los daños y perjuicios que el consumo de bienes o la utilización de productos o servicios hubiera causado a «[t]odo consumidor y usuario»¹⁵⁴. Sin embargo, se llegaría a una conclusión distinta si se siguiera la tesis de BERCOVITZ RODRÍGUEZ-CANO. Según este autor, puesto que los arts. 25 a 27 LGDCU se referían explícitamente a los daños y perjuicios de los consumidores y usuarios, había que excluir de su ámbito de aplicación los daños y perjuicios sufridos por terceros. En cambio, en el caso del art. 28 LGDCU se hablaba de los daños originados en el correcto uso y consumo de bienes y servicios, sin especificar sujeto alguno, por lo que debía extenderse la protección a posibles terceros perjudicados¹⁵⁵.

Esta es, desde luego, la solución más deseable, ya que permitiría proteger a cualesquiera perjudicados por la prestación del servicio defectuoso y no solamente quienes sean, además, usuarios en el sentido del art. 3 TRLGDCU. Y según lo dicho, no debería cambiar el sentido de la norma el hecho de que el vigente art. 148.1 mencione al consumidor y usuario en la cláusula general¹⁵⁶. No obstante, son varios los autores que consideran que el perjudicado por un servicio sanitario ha de ser necesariamente el usuario¹⁵⁷. Ciertamente, en este concepto puede incluirse al paciente o usuario de un servicio sanitario¹⁵⁸, como de hecho reitera la jurisprudencia¹⁵⁹, pero no otros posibles perjudica-

¹⁵⁴ DÍEZ-PICAZO Y PONCE DE LEÓN, L., *Derecho de daños*, Civitas, Madrid, 1999, p. 143; PARRA LUCÁN, M.^a Á., *La protección...*, cit., p. 229; JORQUI AZOFRA, M., *Responsabilidad civil...*, cit., p. 140.

¹⁵⁵ BERCOVITZ RODRÍGUEZ-CANO, R., «La responsabilidad...», cit., p. 232. PANIZA FULLANA, A., «La responsabilidad civil...», cit., p. 16, afirmó, asimismo, que parecía lógico extender la protección del art. 28 LGDCU a los *bystanders*, es decir a aquellos sujetos que, no siendo consumidores, resultan perjudicados por un producto o servicio.

¹⁵⁶ En este sentido, CAVANILLAS MÚGICA, S., «El Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias», *Aranzadi Civil*, núm. 1, abril 2008, p. 44, y PERTÍÑEZ VÍLCHEZ, F., «Disposiciones comunes en materia de responsabilidad», en *La defensa de los consumidores y usuarios*, dir. por Rebollo Puig, M. e Izquierdo Carrasco, M., Iustel, Madrid, 2011, pp. 1812-1813, que defienden que el aparente ensanchamiento del círculo de protegidos se ajusta a los límites de una actuación refundidora porque, en su opinión, la inclusión de los terceros no consumidores podía lograrse mediante una interpretación/integración del antiguo texto legal.

¹⁵⁷ Entre otros, MARTÍN CASALS, M. y SOLÉ FELIU, J., «¿Refundir o legislar?...», cit., p. 92; y SANTOS MORÓN, M.^a J., «La imputación...», cit., p. 122.

¹⁵⁸ El art. 3 de la ya citada Ley 41/2002 sobre autonomía del paciente distingue entre paciente y usuario. El «paciente» se define como la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de la salud, mientras que se considera «usuario» a la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

¹⁵⁹ En este sentido, SSTs núm. 604/1997 1 julio (RJ 5471), 1136/1999 30 diciembre 1999 (RJ 9496), 642/2001 19 junio 2001 (RJ 4974) y 446/2019 18 julio 2019 (RJ 3471), que, en relación con

dos, como podrían ser los acompañantes de los pacientes o usuarios que, por ejemplo, contrajeran una infección hospitalaria como consecuencia de una bacteria ambiental.

5. RESPONSABILIDAD PATRIMONIAL DE LA ADMINISTRACIÓN SANITARIA

Los daños causados en centros sanitarios u hospitales públicos dan lugar a la responsabilidad patrimonial de la Administración, consagrada por el art. 106.2 de la Constitución Española¹⁶⁰ y actualmente regulada, en sus aspectos sustantivos, por la anteriormente mencionada Ley 40/2015 (LRJSP), que sustituye -con carácter continuista- a la anterior Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante, LRJAP). De los aspectos procesales se ocupa la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), que integra el procedimiento de responsabilidad patrimonial, de acuerdo con lo señalado en su Exposición de Motivos, como una especialidad del procedimiento administrativo común, si bien con algunas especialidades¹⁶¹.

Pues bien, de acuerdo con el art. 32 Ley 40/2015, la Administración responde de los «daños causados por el funcionamiento normal o anormal de los servicios públicos», con independencia, al menos aparentemente, de toda culpa individual o institucional.

En efecto, sobre el papel se trata de una responsabilidad objetiva, como recuerda la Sala de lo Contencioso-Administrativo del TS, entre otras muchas, en las sentencias 1806/2020, de 21 diciembre¹⁶² y 232/2022, de 23 febrero¹⁶³, que «surge con el perjuicio que se causa, independientemente de que éste se haya debido a una actuación lícita o ilícita de los Poderes públicos, y de quién haya sido

el art. 1 LGDCU, declararon que la «persona física» que utiliza unos «servicios» «reúne la condición de «usuario» “cualquiera que sea la naturaleza pública o privada, individual o colectiva de quienes los producen, facilitan, suministran o expiden».

¹⁶⁰ De acuerdo con este precepto, «[l]os particulares, en los términos establecidos por la ley, tendrán derecho a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos».

¹⁶¹ TOLOSA TRIBIÑO, C., «La responsabilidad patrimonial de la Administración», *Abogacía española. Consejo General*, 14 marzo 2024, <https://www.abogacia.es/actualidad/opinion-y-analisis/la-responsabilidad-patrimonial-de-la-administracion/>

¹⁶² RJ 2020\5615.

¹⁶³ ECLI:ES:TS:2022:818.

concretamente su causante»; y que se fundamenta, no solamente en el principio de solidaridad («en cuanto no sería justo que un sólo sujeto lesionado tuviera que hacer frente a las consecuencias lesivas de los actos de los Poderes públicos») y en la confianza legítima que los citados Poderes han podido crear en los ciudadanos, sino que también «es, hoy día, una consecuencia obligada e imprescindible del desarrollo del Estado de Derecho que impone la sumisión de la Administración Pública, como a cualquier otro sujeto de Derecho, al ordenamiento jurídico, tal y como se deduce de los artículos 9.3, 103.1, 106.2 o 121 de la Constitución Española de 1978 (CE). La responsabilidad patrimonial, pues, es, hoy, algo más que un mecanismo de compensación de los perjuicios inferidos a concretos ciudadanos por las más diversas actuaciones -no solo administrativas- de las diferentes Administraciones (que deben servir “con objetividad los intereses generales”), y de los distintos Poderes públicos (que están obligados a “promover las condiciones para que la libertad y la igualdad del individuo... sean reales y efectivas”); insistimos, pues, en que, hoy día, la responsabilidad patrimonial es algo más, pues constituye, uno de los pilares fundamentales, junto con el sistema del control jurisdiccional contencioso-administrativo, en la construcción del Derecho administrativo como un Derecho que permite la correcta actuación administrativa bajo el control de los Tribunales de Justicia».

Sin embargo, esta afirmación de la responsabilidad objetiva de la Administración, que se ha convertido en una cláusula de estilo en la jurisprudencia, no se compadece con la realidad de la responsabilidad patrimonial sanitaria¹⁶⁴. En efecto, los tribunales buscan con frecuencia una anormalidad en el funcionamiento del servicio para imputar los daños a la Administración, a fin de evitar que las administraciones públicas se conviertan en aseguradoras universales de cualquier daño que se produzca en la prestación del servicio; si bien, como se encuentran constreñidos por la letra de la ley, justifican sus decisiones ubicando la culpa por infracción de la *lex artis*, no en el ámbito de la imputación subjetiva, sino en el de la relación de causalidad o la antijuridicidad del daño¹⁶⁵. Así, si la asistencia sanitaria ha sido correcta, en ocasiones

¹⁶⁴ Así lo apuntan, entre otros, ASÚA GONZÁLEZ, C., «Responsabilidad civil médica», en Reglero Campos, L. F./Busto Lago, J. M. (coordinadores), *Tratado de Responsabilidad Civil*, vol. II, 5ª. ed., Thomson Reuters-Aranzadi, 2014, pp. 391 y ss., y «Aplicación de la doctrina de la pérdida de oportunidad en la responsabilidad sanitaria», en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón*, coord. por Ataz López, J. y Cobacho Gómez, J. A., tomo II, Thomson Reuters Aranzadi, Cizur Menor (Navarra), p. 466; EGUSQUIZA BALMAEDA, M.^a Á., «Pérdida de oportunidad por retraso diagnóstico. Algunas cuestiones desde la perspectiva jurisprudencial de la responsabilidad patrimonial», en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón*, coord. por Ataz López, J. y Cobacho Gómez, J. A., tomo II, Thomson Reuters Aranzadi, Cizur Menor (Navarra), pp. 256-257.

¹⁶⁵ Entre otros, RODRÍGUEZ LÓPEZ, P., *Responsabilidad patrimonial de la administración en materia sanitaria*, Atelier, Barcelona, 2007, pp. 52-53; ESPINOSA FERNÁNDEZ, F., «Objeto, fundamento y naturaleza jurídica de la responsabilidad patrimonial de la Administración por asistencia sanitaria»,

se declara que el daño sufrido por la víctima no fue causado por dicho funcionamiento, mientras que en otras se estima que dicho daño no es antijurídico y, por tanto, aquella tiene el deber de soportarlo¹⁶⁶. Es evidente que, se formule como se formule, esto implica introducir el criterio de la culpa en una responsabilidad que legalmente es objetiva -como destacó el Magistrado Ollero Tassara en su voto particular a la STC 112/2018, de 17 de octubre¹⁶⁷- y, desde un punto de vista dogmático, no parece correcto; sin embargo, desde un punto de vista práctico, se señala que quizá no pueda ser de otro modo para imponer ciertas dosis de racionalidad en el sistema de responsabilidad patrimonial de la Administración¹⁶⁸. Esto es especialmente así en el caso de la responsabilidad de la Administración sanitaria, teniendo en cuenta que dicha responsabilidad comprende tanto los daños procedentes de aspectos organizativos y funcionales (procedimientos de ambulancia, medios y material quirúrgico...) como los causados por los profesionales sanitarios (médicos, enfermeros, técnicos sanitarios, auxiliares de clínica...) ¹⁶⁹.

A ello responde también la introducción de los «riesgos del progreso» o «riesgos del desarrollo», esto es, los daños procedentes de circunstancias no previsibles o evitables según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de producción de aquellos, como causa de exoneración de responsabilidad por obra de la modificación del art. 141.1 LRJPAC por la Ley 4/1999. Esta previsión, recogida hoy en el art. 34.1 LRJSP, supuso la consagración legal en este ámbito (ya existía en el de productos defectuosos en virtud de la Ley 22/1994) de la doctrina de la Sala 3ª del TS

en *Manual sobre Responsabilidad Sanitaria*, dir. por J. de Fuentes Bardají, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2009, p. 167; MEDIAVILLA CABO, J. V., «Consideraciones sobre la responsabilidad de la administración pública sanitaria tras la crisis derivada del COVID 19», *Revista de Derecho vLex*, núm. 191, abril 2020, pp. 4-5.

¹⁶⁶ Junto con la *lex artis*, se hace referencia también a la *lex scientiae*, entendida como la necesidad de que la prestación sanitaria sea conforme con el estado de los conocimientos de la ciencia y de la técnica. Así, ambas se vinculan al elemento de la antijuridicidad del daño, de manera que allí donde ambos parámetros hayan sido cumplidos no cabe hablar de daño antijurídico, puesto que ni existe obligación de indemnizar los daños que el perjudicado tenga el deber jurídico de soportar, ni tampoco aquellos que no hubieran podido preverse o evitarse de acuerdo con el estado de los conocimientos de la ciencia y de la técnica al tiempo de producirse, esto es, los llamados «riesgos del progreso» (GONZÁLEZ GONZÁLEZ, E., «Administración sanitaria y responsabilidad por productos sanitarios defectuosos con marchamo CE», *REDA*, núm. 200/2019, p. 6).

¹⁶⁷ ECLI:ES:TC:2018:112 (BOE núm. 280, de 20 de noviembre de 2018). A juicio del citado magistrado, en el ámbito sanitario las invocaciones al mayor o menor respeto de sus protagonistas a las exigencias de la llamada *lex artis* no dejan de implicar «un modo solapado de dar entrada a criterios de culpa».

¹⁶⁸ ESPINOSA FERNÁNDEZ, F., «Objeto, fundamento...», cit., p. 162. En la misma línea, ASÚA GONZÁLEZ, C., «Aplicación de...», cit., p. 466.

¹⁶⁹ GARCÍA RUBIO, F. y FUENTES I GASÓ, J. R., *La responsabilidad de las Administraciones Públicas tras la nueva Ley de Régimen Jurídico del Sector Público*, Atelier, Barcelona, 2017, p. 120.

sobre los «riesgos del progreso», la cual asocia esta cuestión con el carácter antijurídico del daño, de modo y manera que cuando la actuación ha sido correcta con arreglo al estado de conocimientos de la ciencia médica al tiempo de los hechos, hay que entender que la lesión no constituye un daño antijurídico y por tanto no es indemnizable¹⁷⁰. Como destacan varios autores, esta reforma -provocada por los problemas que suscita la imputación de los daños con base en el criterio del funcionamiento normal de la Administración¹⁷¹ y que supuso un paso «tímido» hacia la limitación de la responsabilidad de la Administración, aún sin llegar a renunciar a los criterios tradicionales de imputación basados tanto en el funcionamiento normal como anormal de los servicios públicos-, significó la introducción del caso fortuito como causa de exoneración y, por tanto, la entrada a la culpa como criterio de imputación, por más que la Exposición de Motivos de la Ley 4/1999 disponga que lo que se hace es precisar la excepción general de fuerza mayor¹⁷².

De acuerdo con lo dicho hasta ahora, cabe concluir que la Administración sanitaria no responderá de forma objetiva. Así se afirma, sin rodeos, en varias sentencias: «[p]ese al carácter objetivo de la responsabilidad patrimonial de la Administraciones públicas, la responsabilidad sanitaria, cuenta con un evidente componente subjetivo, que le aproxima a la responsabilidad por culpa del art. 1902 del Código Civil, y el parámetro de comprobación es el “incumplimiento de la *lex artis ad hoc*”»¹⁷³.

¹⁷⁰ Véase, al respecto, ESTER CASAS, V., «El concepto de la *lex artis* y su relevancia en la determinación de la relación de causalidad», en *Manual sobre Responsabilidad Sanitaria*, dir. por J. de Fuentes Bardají, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2009, pp. 219 y ss.

¹⁷¹ Muy criticado por la doctrina civilista y por parte de la administrativista, aunque otro sector de esta alaba el sistema, calificándolo como vanguardista. Véase, al respecto, PANTALEÓN PRIETO, F., «Cómo repensar la responsabilidad civil extracontractual (también la de las Administraciones Públicas)», en *Perfiles de la responsabilidad civil en el nuevo milenio*, coord. por J. A. Moreno Martínez, Dykinson, Madrid, 2000, pp. 455 y ss.; ATIENZA NAVARRO, M.^a L., *La responsabilidad civil por los hechos dañosos de los alumnos menores de edad*, Comares, Granada, 2000, pp. 265 y ss.; y LÓPEZ CANDELA, J. E., «El ámbito objetivo de la responsabilidad patrimonial de la Administración por funcionamiento normal con especial mención al servicio sanitario», *Revista Jurídica de Castilla y León*, núm. 15, mayo 2008, p. 97.

¹⁷² DÍEZ-PICAZO Y PONCE DE LEÓN, L., *Derecho de...*, cit., pp. 61 y 62; PANTALEÓN PRIETO, F., «Cómo repensar...», cit., p. 201; ATIENZA NAVARRO, M.^a L., *La responsabilidad civil...*, cit., pp. 261 a 275; DÍAZ-REGAÑÓN GARCÍA-ALCALÁ, C., *Responsabilidad objetiva y nexo causal en el ámbito sanitario*, Comares, Granada, 2006, pp. 209 y ss.

En la legislación de consumo, en cambio, como se ha visto *supra*, no se contemplan los riesgos del desarrollo como causa de exoneración por daños causados por servicios sanitarios, provocando, como también destaca DÍAZ-REGAÑÓN GARCÍA-ALCALÁ, C., *Responsabilidad objetiva...*, cit., p. 86, que la protección del consumidor quede disminuida cuando reclame ante la Administración sanitaria, salvo que se defienda la tesis de excluir la responsabilidad por riesgos de desarrollo también en el contexto del art. 148 TRLGDCU.

¹⁷³ Entre otras, las de la Sala de lo Contencioso 338/2021, de 28 enero, ECLI:ES:TS:2021:338; 2431/2021, de 9 junio, ECLI:ES:TS:2021:2431; 765/2022, de 3 de marzo, ECLI:ES:TS:2022:765.

Aplicando lo anterior a los daños causados por un producto sanitario defectuoso (o aplicado de acuerdo con una información errónea ofrecida por el propio fabricante), como puede ser un SIA utilizado en el tratamiento de un paciente en un hospital público, la Administración no responderá cuando no se pueda probar la culpa del personal médico, sobre todo teniendo en cuenta que dicho producto sanitario goza de la «presunción» de producto apto para el tratamiento del paciente, ya que se trata de un producto que ha pasado una «evaluación de conformidad» recibiendo el plácet de un organismo autorizado en la UE. Si el servicio médico ha utilizado el producto sanitario defectuoso de acuerdo con las exigencias de la *lex artis* no se puede imputar responsabilidad alguna al servicio médico; dicha responsabilidad debe recaer, en todo caso, sobre el fabricante o sobre el organismo encargado de autorizar su uso y/o velar por su adecuado funcionamiento una vez ya puesto en circulación¹⁷⁴. Así lo defiende la Sala Tercera del TS desde la Sentencia de 1806/2020 de 21 diciembre¹⁷⁵, siendo ya doctrina consolidada la de que «la Administración sanitaria -cuyos facultativos realizan correcta y adecuadamente una intervención quirúrgica de conformidad con la *lex artis*- no debe responder de las lesiones causadas a un paciente como consecuencia de la utilización de un producto sanitario defectuoso, cuya toxicidad se descubre y alerta con posterioridad a su utilización, previamente autorizada por la Agencia Española de Medicamentos y Productos Sanitarios, debiendo la responsabilidad recaer en el productor o, en su caso, en la Administración con competencias para autorizar y vigilar los medicamentos y productos sanitarios, de concurrir las concretas circunstancias necesarias para ello»¹⁷⁶.

Por el contrario, si ha concurrido culpa en la prestación del servicio médico en el que se ha utilizado un producto sanitario defectuoso, la Administración sanitaria sí que puede ser responsable por los daños causados al paciente por ese producto sanitario defectuoso (los guantes están en mal estado y aun así se usan y ello provoca una infección en el paciente; el producto sanitario da unos resultados anómalos atendidas las circunstancias y aun así no se indaga en el porqué de dichos resultados; el producto sanitario ya había provocado problemas en otras ocasiones y aun así se sigue utilizando sin más, etc.)¹⁷⁷. Una vez satisfecha la indemnización procedente, la Administración correspondiente exigirá de

¹⁷⁴ GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 11.

¹⁷⁵ ECLI:ES:TS:2020:4495.

¹⁷⁶ Ver, por todas, SSTs (Sala de lo Contencioso) 765/2022 de 3 marzo, ECLI:ES:TS:2022:765, y 3581/2022 de 6 octubre, ECLI:ES:TS:2022:3581. En la misma línea, asimismo, las sentencias de la misma Sala del TS núm. 219/2021, de 21 enero, ECLI:ES:TS:2021:219; 338/2021, de 28 enero, ECLI:ES:TS:2021:338; 2431/2021 de 9 junio, ECLI:ES:TS:2021:2431; 4317/2021 de 17 noviembre, ECLI:ES:TS:2021:4317; 4521/2021 de 1 diciembre, ECLI:ES:TS:2021:4521; 818/2022 de 23 febrero, ECLI:ES:TS:2022:818.

¹⁷⁷ GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 11.

oficio en vía administrativa del personal a su servicio –al que no se puede demandar directamente por el perjudicado– la responsabilidad en que hubieran incurrido por dolo o culpa graves (art. 36.2 LRJAP).

Asimismo, la responsabilidad de la Administración sanitaria puede proceder de un mal mantenimiento del producto sanitario (por ejemplo, no proceder a las revisiones previstas por el fabricante), de no revisar si el producto sanitario ha caducado, de no almacenarlo en un lugar adecuado, etc. En este caso, aparte de los arts. 32 y ss. LRJAP, cabría también aplicar el art. 148 TRLGDCU, de acuerdo con la doctrina del TS, pues esta actividad descrita no es un «acto médico» pero sí que parece que puede incluirse entre los «aspectos funcionales del servicio»¹⁷⁸.

6. RÉGIMEN DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL DEL CÓDIGO CIVIL

En todos aquellos casos no cubiertos por los regímenes especiales de responsabilidad objetiva a los que me he referido, habrá que acudir a las reglas generales de responsabilidad del CC.

Así, por ejemplo, para solicitar una indemnización al fabricante por daños causados por un producto defectuoso no incluidos en el ámbito de aplicación de la normativa sobre productos defectuosos (pérdidas puramente económicas, discriminación, daños a derechos de la personalidad, daños a bienes usados de forma profesional, daños al medio ambiente...); o para exigir responsabilidad civil a los profesionales sanitarios por su actuación médica. Esta responsabilidad puede ser contractual (arts. 1101 y ss.) o extracontractual (art. 1902 CC). La segunda surge cuando infringen la *lex artis ad hoc* (ley del arte), definida por el TS como el «el conjunto de conocimientos, técnicas y habilidades aplicables en un concreto sector de la actividad humana»¹⁷⁹, como el de la medicina¹⁸⁰. La *lex artis* representa un estándar de diligencia

¹⁷⁸ GRIMALT SERVERA, P., «La responsabilidad...», cit., p. 11.

¹⁷⁹ STS (Sala de lo Civil) 20250/2023, de 8 mayo, ECLI:ES:TS:2023:2050. En términos parecidos, la STS (Sala de lo Contencioso) 3106/2020, de 30 septiembre, ECLI:ES:TS:2020:3106: «conjunto de reglas técnicas a que ha de ajustarse la actuación de un profesional en el ejercicio de su arte u oficio».

¹⁸⁰ De acuerdo con la STS 778/2009, de 20 de noviembre, «[e]n el caso de la asistencia médica, la *lex artis* abarca la utilización de los medios y técnicas necesarias, que el estado actual de conocimientos de la medicina, posibilita para el diagnóstico de las enfermedades, de manera proporcional al cuadro clínico que presenta el enfermo; seguir las prevenciones aceptadas por la comunidad científica para el tratamiento de la patología padecida; la práctica diligente de las técnicas empleadas en el proceso curativo, comprendiendo las quirúrgicas; la prestación de la información precisa, con antelación temporal suficiente, de manera comprensible, sobre el diagnóstico, pronóstico, tratamiento, riesgos típicos y prevenciones a seguir en el proceso de curación de la enfermedad; abstenerse de

exigible más elevado que la clásica diligencia del «buen padre de familia», o en terminología más moderna, de la «persona prudente y razonable» en las mismas circunstancias¹⁸¹; y está compuesta, no solo por reglas jurídicas, sino también por las de carácter ético o moral que forman el código deontológico o de conducta profesional¹⁸², así como por los protocolos médicos, que recogen las recomendaciones que, salvo mejor criterio en contemplación de las peculiaridades del caso, la comunidad científica tiene establecidas en cuanto al diagnóstico y respuesta terapéutica ante determinadas circunstancias clínicas que presentan ciertas patologías¹⁸³.

En lo que a la responsabilidad médica por daños causados con ocasión del uso de sistemas inteligentes, conviene distinguir entre los SIA que se utilizan como asistentes y los que sustituyen la decisión humana. De acuerdo con un sector doctrinal, solamente en el primer caso (como, p. ej., cuando se usa un robot quirúrgico tipo *Da Vinci*, un asistente para diagnóstico o tratamiento o una app de salud) podrá aplicarse la responsabilidad por hecho propio del art. 1902 CC, que exige la culpa o negligencia del facultativo (y que, en su caso, puede acumularse a la responsabilidad del productor si el SIA es un producto defectuoso¹⁸⁴). Otros, en cambio, a partir de la propuesta de crear un sistema de responsabilidad por culpa en cascada por los daños causados por los robots, defienden que el formador de un sistema inteligente debe responder por culpa *in educando* cuando haya sido negligente al formar a la herramienta. Y se pone el ejemplo de las IA de reconocimiento fotográfico, que precisan de un entrenamiento al objeto de aprender de forma autónoma y heterónoma a examinar imágenes y clasificarlas. Se dice, en relación con ello, que «[s]i un robot, en perfecto estado de mantenimiento de sus senso-

actuar en contra o al margen del consentimiento informado del paciente, que habrá de obtenerse, con mayor rigor, en el caso de la medicina voluntaria o satisfactiva; cumplimentar los deberes de la documentación clínica, sin incurrir en omisiones relevantes e injustificadas; y actuar siempre, de forma diligente, mediante el control de las incidencias del curso de la patología, sin incurrir en descuidos inasumibles, hasta el alta del paciente, con las indicaciones correspondientes de seguimiento, si fueran procedentes (prevenciones pautadas y revisiones periódicas en su caso)».

¹⁸¹ Art. 4:102 *Principles of European Tort Law* (PETL); Art. VI-3:102 *Draft of Common frame of Reference* (DCFR), citados por SOLÉ FELIU, J., «Estándar de diligencia médica y valor de los protocolos y guías de práctica clínica en la responsabilidad civil de los profesionales sanitarios», *Revista de Derecho Civil*, vol. IX, núm. 3 (julio-septiembre, 2022), p. 2, quien menciona también, en la misma línea, el art. 5191-8(1) del Proyecto de Código Civil promovido por la Asociación de Profesoras y Profesores de Derecho Civil, según el cual «[E]s contraria al deber de diligencia exigible toda acción u omisión que se aparta de lo que haría una persona cuidadosa y prudente en las mismas circunstancias».

¹⁸² STS 5 diciembre 2006, RJ 2007/232.

¹⁸³ GALLARDO CASTILLO, M.^a J., *Administración sanitaria y responsabilidad patrimonial*, Colex, A Coruña, 2021, pp. 34-35.

¹⁸⁴ ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 368; ALKORTA, I., «Five crucial challenges...», cit., p. 12.

res, como consecuencia de un defecto formativo, que no de programación, identifica de forma errónea una determinada figura de la realidad materiales, desembocando dicha identificación equivocada, en daño a una persona, habrán de responder los formadores»¹⁸⁵.

Recuérdese, además, que aun en los casos en que el SIA sea el que actúe o tome una decisión, de acuerdo con el art. 14 RIA, debe diseñarse y desarrollarse de manera que permita una vigilancia efectiva por personas físicas durante el periodo de su utilización¹⁸⁶ y que la PDRIA considera acreditada la culpa del usuario profesional cuando el demandante demuestre que aquel: a) No cumplió con sus obligaciones de utilizar o supervisar el sistema inteligente de conformidad con las instrucciones de uso adjuntas o, en su caso, de suspender o interrumpir su uso con arreglo al art. 26 RIA (esto es, cuando tenga motivos para considerar que utilizar el sistema inteligente conforme a sus instrucciones de uso podría hacer que aquel presentase un riesgo o cuando detecte un incidente grave o un defecto de funcionamiento); o b) Expuso al sistema de inteligencia artificial a datos de entrada bajo su control que no eran pertinentes habida cuenta de la finalidad prevista del sistema con arreglo al art. 26 RIA. Teniendo en cuenta que, como indica el cdo. 15 PDRIA, sus previsiones se aplican a los procedimientos relativos a responsabilidad civil extracontractual por daños causados directamente por sistemas inteligentes, y no a aquellos en que los daños hayan sido causados por una evaluación humana seguida de una acción u omisión humana y el sistema inteligente se haya limitado a proporcionar información o asesoramiento que fue tenido en cuenta por el agente humano de que se trate (precisamente porque son los primeros supuestos los que necesitan regulación específica, y no los segundos, dado que en estos, «es posible atribuir los daños causados a una acción u omisión humana, ya que la información de salida del sistema de IA no se interpone entre la acción u omisión humana y el daño, por lo que establecer la causalidad no es más difícil que en situaciones en las que no interviene un sistema de IA»), creo que la conclusión de que el profesional sanitario no responderá cuando los SIA sustituyan la decisión humana es, quizá, precipitada.

Volviendo a las aplicaciones usadas por los médicos como apoyo de sus propias decisiones, a los efectos de determinar la negligencia del profesional sanitario, entiendo que no la habrá en aquellos casos en los que haya confiado en el diagnóstico elaborado y/o el tratamiento prescrito de forma errónea

¹⁸⁵ ERCILLA GARCÍA, J., «Aproximación a una Personalidad Jurídica Específica para los robots», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 47, 2018, pp. 19-20.

¹⁸⁶ Incumplir este deber, además, por el proveedor de un SIA de alto riesgo o sujeto asimilado según el RIA, implicará la culpa de este a los efectos de la presunción de causalidad entre la acción u omisión culposa del demandado y los resultados producidos por el SIA o la no producción de resultados por parte de este prevista en el art. 4 PDRIA.

por el sistema inteligente tras un análisis diligente del resultado. En efecto, la evaluación de la negligencia del facultativo deber conforme a la *lex artis ad hoc*, de manera que no quedará exonerado de responsabilidad cuando, sin control ni revisión alguna, haya dado por buena la decisión del sistema inteligente sin más. En cualquier caso, cuando el daño ha sido causado, no por negligencia del facultativo, sino por un defecto del SIA utilizado por aquel, no habrá responsabilidad del médico, sino del productor, con base en la normativa sobre responsabilidad civil por daños causados por productos defectuosos, así como del centro sanitario público o privado en el que el médico presta sus servicios, con base en el art. 32 Ley 40/2015 o el art. 148 TRLGDCU, respectivamente.

¿Qué pasará, en cambio, en la hipótesis de que el médico decida apartarse del diagnóstico hecho y/o el tratamiento prescrito por el sistema inteligente y el paciente sufra daños por ello? Sobre la base del escaso número de errores que cometen estos sistemas, ciertos autores afirman que probablemente haya que entender que en este caso habría culpa del médico y que, por tanto, prosperaría una demanda basada en la «pérdida de oportunidad»¹⁸⁷; lo cual implica, en definitiva, modificar la forma de valorar la negligencia médica, hasta ahora basado en comparar la decisión del facultativo con la de otro que hubiera utilizado las reglas de la *lex artis ad hoc*, introduciendo un nuevo *standard* de conducta, consistente en comparar con la decisión de un SIA¹⁸⁸. Por el contrario, no se considera negligente la conducta del médico que, sin tener a su alcance un asistente inteligente, concluye de forma distinta a cómo lo habría hecho este; ni tampoco se estima defendible que el hospital deba responder por no utilizar esos sistemas de inteligencia artificial por el hecho de resultarle económicamente costosos¹⁸⁹. Personalmente creo que debe estarse a las circunstancias del caso concreto, sin que el hecho de que el facultativo se aparte del diagnóstico hecho y/o el tratamiento prescrito por el sistema inteligente y el paciente sufra daños por ello deba implicar, necesariamente, una negligencia médica¹⁹⁰.

¹⁸⁷ ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 372.

¹⁸⁸ BERTOLINI, A., *Artificial intelligence and civil liability* (estudio encargado por la Comisión de Asuntos Jurídicos del Parlamento Europeo), julio 2020, disponible en [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf), p. 114; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 372.

¹⁸⁹ MONTERROSO CASADO, E. y DÍAZ DÍAZ, E., «La responsabilidad civil...», cit., p. 125; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., p. 373.

¹⁹⁰ Ni siquiera en el caso de que el uso de determinados sistemas inteligentes se incluya en los protocolos aplicables, como probablemente acabe ocurriendo, puesto que los protocolos, como subraya GALLARDO CASTILLO, M.^a J., *Administración sanitaria...*, cit., p. 35, si bien ofrecen al juzgador un importante elemento de juicio, y el apartamiento de lo previsto en el protocolo requiere de una justificación rigurosa, no son determinantes en la evaluación de la diligencia médica, la cual debe hacerse tomando siempre en consideración, como se ha señalado, las singularidades de todo orden presentes en cada actuación médica.

En cualquier caso, la responsabilidad del médico que hubiera incurrido en alguna violación de las normas de la *lex artis* solo podrá exigirse cuando desempeñase sus funciones en un centro privado; en el caso de que fuera público, como ya se ha visto, solamente podría reclamarse a la Administración, la cual, una vez que haya indemnizado al perjudicado, exigirá de oficio en vía administrativa del médico a su servicio la responsabilidad en que hubiera incurrido por dolo o culpa grave (art. 36 Ley 40/2015¹⁹¹). Ahora bien, volviendo a la hipótesis de daño causado por negligencia de un profesional médico que presta sus servicios en un centro privado, siguiendo la doctrina consolidada del TS en el sentido de que los servicios sanitarios a los que se refiere el art. 148 TRLGDCU no incluyen la prestación médica en sí misma, sino exclusivamente los aspectos funcionales y organizativos del servicio, no cabrá en este caso hacer responder (objetivamente) al centro privado por daños causados por negligencia médica de sus facultativos. Otra cosa es que dicha responsabilidad se reclame por la vía del art. 1903.5 CC.

Llegados a este punto, cabe recordar que el régimen de responsabilidad por culpa por daños causados por sistemas de IA se verá afectado, en caso de que su tramitación siga adelante, por la ya mencionada Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de inteligencia artificial) de 28 de septiembre de 2022, en aquellos aspectos por esta regulados, que, a pesar de su denominación, únicamente se refieren a la carga de la prueba. En efecto, la Propuesta no armoniza «los aspectos generales de la responsabilidad civil que estén regulados de diferentes maneras por las normas nacionales de responsabilidad civil, como la definición de la culpa o la causalidad, los diferentes tipos de daños que dan lugar a demandas por daños y perjuicios, la distribución de la responsabilidad entre varios causantes de los

En relación con ello, GIL MEMBRADO, C., *Riesgos del uso...*, cit., p. 170, afirma, con razón, que en el caso de sistemas inteligentes, puede ser imposible para el facultativo justificar por qué se aparta del resultado del sistema, por el conocido efecto de caja negra.

¹⁹¹ En efecto, según el apartado 1 de dicho precepto, «[p]ara hacer efectiva la responsabilidad patrimonial a que se refiere esta Ley, los particulares exigirán directamente a la Administración Pública correspondiente las indemnizaciones por los daños y perjuicios causados por las autoridades y personal a su servicio». A ello añade el apartado 2 lo siguiente: «La Administración correspondiente, cuando hubiere indemnizado a los lesionados, exigirá de oficio en vía administrativa de sus autoridades y demás personal a su servicio la responsabilidad en que hubieran incurrido por dolo, o culpa o negligencia graves, previa instrucción del correspondiente procedimiento.

Para la exigencia de dicha responsabilidad y, en su caso, para su cuantificación, se ponderarán, entre otros, los siguientes criterios: el resultado dañoso producido, el grado de culpabilidad, la responsabilidad profesional del personal al servicio de las Administraciones públicas y su relación con la producción del resultado dañoso».

daños, la concurrencia de culpas, el cálculo de los daños y perjuicios o los plazos de prescripción»¹⁹².

Esta solución adoptada por la PDRIA es acorde con el sentir mayoritario de las instancias europeas y los grupos de trabajo en relación con tres puntos: a) La no necesidad de realizar una revisión completa y exhaustiva de las normas generales sobre responsabilidad civil en la UE para lograr que las víctimas de daños ocasionados por sistemas inteligentes obtengan adecuada protección¹⁹³; b) El reconocimiento de la dificultad de armonización, dada la gran disparidad entre legislaciones en esta materia¹⁹⁴; y c) La búsqueda de proporcionalidad entre la protección de los perjudicados y el desarrollo de la inte-

¹⁹² Según se puede leer en la E. de M., p. 7, y los cdos. 9 y 10 de la PDRIA, la CE no considera necesario ni conveniente armonizar esos aspectos, estimando que la armonización de ciertos aspectos de la carga de la prueba es suficiente para aumentar la seguridad jurídica y crear unas condiciones de competencia equitativas para los sistemas inteligentes, mejorando así el funcionamiento del mercado interior en lo que respecta a la producción y difusión de productos y servicios basados en la inteligencia artificial.

¹⁹³ VOSS, A., *Draft report on artificial intelligence in a digital age*, 2020/2266 (INI), Special Committee on artificial intelligence in a digital age, 2.11.2021, p. 28, cdo. 131. También en la doctrina tiene un peso relevante esta opinión. *Vid.*, en este sentido, EBERS, M., «La utilización...», cit., p. 8; RUBÍ PUIG, A., «Retos de la...», cit., pp. 58 y 63; KOCH, B./BORGHETTI, J. B./MACHNIKOWSKI, P./PICONNAZ, P./RODRÍGUEZ DE LAS HERAS BALLELL, T./TWIGG-FLESNER, C./WENDEHORST, C., *Response of the...*, cit., p. 11.

No obstante, también hay autores que defienden el establecimiento de un nuevo régimen de responsabilidad civil para inteligencia artificial y robótica. En esta línea, AZNAR DOMINGO, A./DOMÍNGUES VILLARROEL, M. P., «La responsabilidad civil derivada del uso de la inteligencia artificial», *ELDerecho.com*, Tribuna, 1 julio 2022, <https://elderecho.com/responsabilidad-civil-derivada-uso-inteligencia-artificial>, quienes abogan por una regulación de carácter sectorial en los diferentes ámbitos; ZURITA MARTÍN, I., «Las propuestas de reforma legislativa del Libro Blanco Europeo sobre Inteligencia Artificial en materia de seguridad y responsabilidad civil», *Actualidad Jurídica Iberoamericana*, n. 14, febrero 2021, p. 477, que asimismo sostiene que la decisión sobre el régimen de responsabilidad más oportuno debe depender del tipo de robot de que se trate; NAVAS NAVARRO, S., «Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial», *Revista CESCO de Derecho de Consumo*, núm. 44/2022, p. 49, para quien «todavía queda espacio para establecer un régimen jurídico propio para la responsabilidad civil por los daños ocasionados por sistemas de IA, quizá en la línea de lo advertido por la resolución del Parlamento europeo de 20 de octubre de 2020, que equipare a las víctimas de daños ocasionados por sistemas de IA con las víctimas de daños ocasionados por productos defectuosos. No se acaba de entender que el estándar sea diferente cuando los daños que puede llegar a ocasionar un sistema de IA pueden ser tanto o más relevantes que los que ocasione un producto que presenta un defecto»; y RAMÓN FERNÁNDEZ, F., «El robot como producto defectuoso y responsabilidad civil», *Derecho Digital e Innovación*, núm. 14, 2022, p. 9, que sostiene que la PDRIA debería haber distinguido según la categoría del sistema de IA y haber contemplado la responsabilidad civil objetiva en el caso de daños por sistemas inteligentes que no fueran de alto riesgo.

¹⁹⁴ KARNER, E./KOCH, B./GEISTFELD, M., *Comparative law study on civil liability for artificial intelligence*, estudio encargado por la Comisión Europea, Dirección General de Justicia y Consumidores, al *European Law Institute (ELI)*, Publications Office, Publications Office, 2021, disponible en: <https://data.europa.eu/doi/10.2838/66412>, pp. 9 y ss., y GIL MEMBRADO, C., «En el horizonte: la Directiva de responsabilidad extracontractual en materia de IA», en Gil Membrado, C. (dir. y coord.), *Derecho y medicina: desafíos tecnológicos y científicos*, Dykinson, Madrid, 2023, p. 116.

ligencia artificial en la UE, que pretende convertirse en referente normativo mundial¹⁹⁵.

Sin embargo, en el mencionado informe de P. HACKER sobre la PDRIA, se sostiene que este texto es insuficiente. En este sentido, se subrayan dos deficiencias relevantes en el debate sobre la AI de la Comisión Europea: un conjunto incompleto de opciones políticas y un análisis abreviado de costes y beneficios de las opciones políticas. En cuanto a la primera, se critica que se presta poca atención a la resolución del Parlamento Europeo de 2020 sobre la responsabilidad por IA, haciendo referencia, concretamente, a que la CE «no investiga a fondo la posibilidad de integrar la responsabilidad objetiva con límites de responsabilidad, y carece de profundidad a la hora de explorar un espectro más amplio de presunciones de negligencia o inversiones completas de la carga de la prueba». Esto conduce, además, en opinión del autor del informe, a que el análisis de la AI de los costes y beneficios asociados a opciones normativas alternativas, como la responsabilidad objetiva, se detalle de forma incoherente; de manera que «[a]unque algunos aspectos de estas opciones normativas están bien examinados, la evaluación se queda bastante corta a la hora de debatir el potencial y los inconvenientes asociados a un régimen de responsabilidad objetiva»¹⁹⁶.

A partir de ahí, el Informe realiza una serie de recomendaciones, que, de seguirse, implicarán cambios relevantes en la tramitación de la Propuesta de Directiva, desde retomar la opción de un reglamento en vez de una directiva, hasta incidir en cuestiones sustantivas, y no solo procesales, sobre la responsabilidad civil por daños causados por sistemas inteligentes. El futuro dirá.

7. CONSIDERACIONES FINALES SOBRE LA CONCURRENCIA DE REGÍMENES APLICABLES

Como se ha visto, la indemnización por daños causados con intervención de sistemas inteligentes puede reclamarse a través de diferentes vías, que pueden ser compatibles entre sí. Así, por ejemplo, de acuerdo con el art. 128.2 TRLGDCU, las acciones de responsabilidad civil por daños causados por productos o servicios defectuosos reconocidas en dicho texto legal «no afectan a

¹⁹⁵ COMITÉ ECONÓMICO Y SOCIAL EUROPEO, *Dictamen sobre Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)* [COM(2022) 496 final - 2022/0303 (COD)] (2023/C 140/05), 25.1.2023, conclusión-recomendación 7.6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=esc%3AEESC-2022-04704>

¹⁹⁶ HACKER, P., *Study about...*, cit., p. I.

otros derechos que el perjudicado pueda tener a ser indemnizado por daños y perjuicios, incluidos los morales, como consecuencia de la responsabilidad contractual, fundada en la falta de conformidad de los bienes o servicios o en cualquier otra causa de incumplimiento o cumplimiento defectuoso del contrato, o de la responsabilidad extracontractual a que hubiere lugar».

Así las cosas, cabe mencionar, sin ánimo de exhaustividad, los siguientes supuestos:

- 1) Usuario de un servicio sanitario que es víctima de un daño provocado por un mal funcionamiento de un sistema inteligente utilizado en la prestación del servicio debido exclusivamente a un defecto del producto. Podrá reclamar al prestador del servicio sanitario (si es privado), con base en el art. 148 TRLGDCU o el 138 TRLGDCU, así como al fabricante del SIA y, en su caso, del *software* incorporado en el SIA, si son sujetos diferentes y si el defecto procede del programa informático, en ambos casos con base en el régimen de RC por daños causados por productos defectuosos. Ahora bien, si el fabricante del *software* presta también servicios técnicos de informática al hospital o centro de salud, se dice que responderá como prestador de servicios¹⁹⁷.

También cabrá exigir responsabilidad, además de a los sujetos contemplados en el régimen especial de responsabilidad de los arts. 135 y ss. TRLGDCU, al hospital público, con base en el art. 32 Ley 40/2015. Otra cosa es que finalmente recaiga condena del prestador del servicio sanitario, como ya se explicó.

Asimismo, tanto en este caso como en cualquier otro en el que el defecto en el producto debería haber activado los deberes de realización de auditorías sin previo aviso del organismo notificado y ello no hubiera ocurrido, este organismo será potencialmente responsable, junto con el productor o asimilado, del daño causado. Además, si la autoridad nacional competente conforme al RPS no hubiera adoptado las medidas de precaución que la citada norma contempla, también será responsable¹⁹⁸.

- 2) Usuario de un servicio sanitario que es víctima de un daño provocado por un mal funcionamiento de un sistema inteligente debido a una incorrecta manipulación del producto. En estos casos, el productor

¹⁹⁷ ZURITA MARTÍN, I., «Las propuestas...», cit., p. 463, que estima que, si bien los servicios informáticos, en su generalidad, no deben considerarse incluidos per se entre los servicios del art. 148 TRLGDCU, sí han de someterse al régimen de este precepto cuando atiendan a los servicios que en él se recogen; ATIENZA NAVARRO, M.^a L., *Daños causados...*, cit., pp. 148-149.

¹⁹⁸ Así lo indica también GARCÍA MICÓ, T. G., *Robótica quirúrgica...*, cit., pp. 132-133.

(o el operador económico) no responderá con base en el régimen de responsabilidad por daños causados por productos defectuosos, sino que debería responder de forma exclusiva la Administración pública responsable del hospital en el que se utiliza un producto que causa daños (con base en el art. 32 Ley 40/2015), quien deberá después repetir de oficio contra el personal a su servicio que haya utilizado incorrectamente el sistema inteligente con culpa grave o dolo (art. 36.2 LRJAP); o si se trata de un hospital privado, en la medida en que este supuesto quedaría excluido del ámbito de aplicación del art. 148 TRLGDCU, el prestador del servicio podría responder con base en el art. 1903.4 CC, previa demostración de la culpa del facultativo, quien también respondería por hecho propio *ex* art. 1902 CC.

- 3) Usuario de un servicio sanitario que es víctima de un daño causado por un mal funcionamiento de un sistema inteligente provocado tanto por un defecto del producto como por causas relacionadas con los aspectos organizativos del servicio o por utilización negligente por el prestador del servicio. En este caso, hay quien defiende que el prestador (privado) del servicio sanitario responderá solidariamente con el productor, de acuerdo con el art. 132 TRLGDCU¹⁹⁹. Sin embargo, esta norma hace responder solidariamente a las personas que sean responsables del mismo daño «por aplicación de este libro», lo que, en el caso del prestador del servicio sanitario, de acuerdo con la interpretación del art. 148 TRLGDCU por el TS, implica responder por los aspectos organizativos y funcionales. Por tanto, entiendo que cuando el daño proceda tanto del defecto del producto como de negligencia médica, aparte de la responsabilidad del productor, podrá exigirse responsabilidad al médico, con base en el art. 1902 CC y al hospital privado *ex* art. 1903.4 CC; en cambio, si se trata de daño causado conjuntamente por defecto del sistema de IA y por un almacenamiento incorrecto, no por parte del facultativo, sino de otro personal del centro, sí habrá responsabilidad solidaria por el art. 132 TRLGDCU.

Si estamos ante un prestador público del servicio sanitario, como se ha visto, la concurrencia de causas entre el defecto del producto y la actuación médica o del personal del hospital puede dar lugar a reclamar tanto a quien sea responsable conforme a los arts. 135 y ss. TRLGDCU cuanto a la Administración pública con base en los arts. 32 y ss. Ley 40/2015.

¹⁹⁹ GÓMEZ LIGÜERRE, C., «Responsabilidad del...», cit., p. 61.

- 4) Usuario de un servicio sanitario que es víctima de un daño causado por un mal funcionamiento de un sistema inteligente provocado tanto por un defecto del producto como por la acción de un tercero (transportista, pirata informático...). En esta hipótesis, el productor (u operador económico según la PDRDPD) seguirá siendo responsable ante el perjudicado, con base en el art. 133 TRLGDCU (y 13 de la Propuesta), sin perjuicio de la acción de repetición contra el tercero. También este podrá ser demandado, con base en el art. 1902 CC. De igual forma, dada la responsabilidad objetiva (con todos sus matices en la práctica) de los prestadores de servicios sanitarios según los arts. 148 TRLGDCU y 132 LRJSP, asimismo estos podrían ser demandados.

En el caso de que el daño fuera causado exclusivamente por la intervención de un tercero, como se ha visto, la ruptura del nexo causal respecto de la acción del productor debe conducir, según el régimen vigente, a la exoneración de este, conforme a las reglas generales de responsabilidad civil. En la PDRDPD, sin embargo, como se ha visto, se excluye dicha exoneración.

La posible concurrencia de diferentes sujetos responsables y, por tanto, de diferentes fundamentos jurídicos para la reclamación de una indemnización plantea cuestiones procesales relativas a la jurisdicción competente. Si bien el análisis en profundidad de este punto excede del propósito de este trabajo, creo que interesa hacer una breve referencia a ello.

Así, centrándonos en el momento actual, y tras muchos años de polémica a este respecto²⁰⁰, de acuerdo con el apartado segundo del art. 9.4 LOPJ, en su vigente redacción, dispone que los juzgados y tribunales del orden contencioso-administrativo conocerán de las pretensiones que se deduzcan en relación con la responsabilidad patrimonial de las Administraciones públicas y del personal a su servicio, cualquiera que sea la naturaleza de la actividad o el tipo de relación de que se derive. Añade el precepto que incluso cuando a la producción del daño hubieran concurrido sujetos privados, «el demandante deducirá también frente a ellos su pretensión ante este orden jurisdiccional»; así como que será competente este orden jurisdiccional cuando el interesado accione directamente contra la aseguradora de la Administración, junto a la Administración respectiva, o cuando las demandas de responsabilidad patrimonial se dirijan, además de contra la Administración, contra las personas o entidades públicas o privadas indirectamente responsables de aquellas.

²⁰⁰ Sobre la evolución legislativa y jurisprudencial al respecto, ver, por todos, GALÁN CORTÉS, J., *Responsabilidad civil...*, cit., pp. 52 y ss.

El art. 35 LRJSP, por su parte, dispone que «[c]uando las Administraciones Públicas actúen, directamente o a través de una entidad de derecho privado, en relaciones de esta naturaleza, su responsabilidad se exigirá de conformidad con lo previsto en los artículos 32 y siguientes, incluso cuando concurra con sujetos de derecho privado o la responsabilidad se exija directamente a la entidad de derecho privado a través de la cual actúe la Administración o a la entidad que cubra su responsabilidad». Aunque el precepto no se refiere a cuestiones jurisdiccionales, ciertos autores entienden que va de suyo que el orden contencioso-administrativo es competente para resolver todas las demandas frente a la Administración pública por responsabilidad patrimonial en las que se reclama también a un sujeto de Derecho privado, e incluso para conocer de las demandas en las que se ejercite exclusivamente la acción directa del art. 76 de la Ley del Contrato de Seguro frente a la aseguradora de la Administración²⁰¹. Otros, en cambio, sostienen que cuando la acción se dirige exclusivamente contra la aseguradora, pese a lo dispuesto por el art. 35 LRJSP, cabe interponer la demanda ante el orden civil, en tanto en cuanto no se modifique el párrafo segundo, último inciso, del art. 9.4 LOPJ, por el mayor rango de esta norma²⁰².

8. BIBLIOGRAFÍA

- ALKORTA, I., «Five crucial challenges for regulation of Medical artificial intelligence», *Revista Internacional de Estudios Vascos*, 67-2, pp. 2-15.
- ÁLVAREZ OLALLA, P., «Daños causados al paciente por utilización de un producto sanitario defectuoso. Al hilo del caso Ala Octa», *RCDI*, núm. 794, 2022, pp. 3366-3405.
- ASÚA GONZÁLEZ, C., «Responsabilidad sin culpa en la medicina privada: el artículo 28 LGDCU», en Moreno Martínez, J. A. (coordinador), *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007, pp. 37-66.
- «Responsabilidad civil médica», en Reglero Campos, L. F./Busto Lago, J. M. (coordinadores), *Tratado de Responsabilidad Civil*, vol. II, 5ª. ed., Thomson Reuters-Aranzadi, 2014, pp. 331-430.
- «Aplicación de la doctrina de la pérdida de oportunidad en la responsabilidad sanitaria», en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón*, coord. por Ataz López, J. y Cobacho Gómez, J. A., tomo II, Thomson Reuters Aranzadi, Cizur Menor (Navarra), pp. 441-468.

²⁰¹ GALLARDO CASTILLO, M.ª J., *Administración sanitaria...*, cit., pp. 57-58.

²⁰² GALÁN CORTÉS, J., *Responsabilidad civil...*, cit., pp. 66 y 72-73.

- ATAZ LÓPEZ, J., «Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial», *Working paper 4/2020*, Working papers Jean Monnet Chair – European Private Law, Universitat de Barcelona, pp. 1-56.
- ATIENZA NAVARRO, M.^a L., *La responsabilidad civil por los hechos dañosos de los alumnos menores de edad*, Comares, Granada, 2000.
- *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022.
- «¿Una nueva responsabilidad por productos defectuosos?», *Indret*, 2, 2023, pp. 1-53.
- «La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 341-409.
- AZNAR DOMINGO, A./DOMINGUES VILLARROEL, M. P., «La responsabilidad civil derivada del uso de la inteligencia artificial», *ElDerecho.com*, Tribuna, 1 julio 2022, <https://elderecho.com/responsabilidad-civil-derivada-uso-inteligencia-artificial>.
- BERCOVITZ RODRÍGUEZ-CANO, R., «La responsabilidad de los fabricantes en la Directiva de las Comunidades Europeas de 25 de junio de 1985», *Estudios sobre consumo*, núm. 7, 1986, pp. 222-247.
- «Comentario a la STS de 1 de julio de 1997», *CCJC*, núm. 45, 1997, pp. 1211-1221.
- BERTOLINI, A., *Artificial intelligence and civil liability* (estudio encargado por la Comisión de Asuntos Jurídicos del Parlamento Europeo), julio 2020, disponible en [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf)
- CÁMARA LAPUENTE, S., *Comentarios a las normas de protección de los consumidores*, Colex, Madrid, 2011.
- CARRASCO PERERA, Á., «A propósito de un trabajo de Gunther Teubner sobre la personificación civil de los agentes de inteligencia artificial avanzada», *Publicaciones Jurídicas CESCO*, 11 de enero de 2019, disponible en https://centrodeestudiosdeconsumo.com/images/A_proposito_de_un_trabajo_de_Gunter_Teubner_.pdf, pp. 1-6.
- CAVANILLAS MÚGICA, S., *Responsabilidad civil y protección del consumidor*, Universitat de les Illes Balears, Palma de Mallorca, 1985.
- «El Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias», *Aranzadi Civil*, núm. 1, abril 2008, pp. 17 a 48.
- CAYÓN DE LAS CUEVAS, J., *La prestación de servicios sanitarios como relación jurídica de consumo*, Civitas Thomson Reuters, Cizur Menor (Navarra), 2017.
- CUETO PÉREZ, M., «Jurisprudencia en el caso ALA OCTA: responsabilidad patrimonial por la utilización de productos defectuosos en el ámbito sanitario», *Revista de Administración Pública*, 217, 2022, p. 172, doi: <https://doi.org/10.18042/cepc/rap.217.05>

- DE BRUYNE, J., VAN GOOL, E. y GILS, T., «Tort law and damage caused by AI systems», en De Bruyne, J./Vanleenhove, C., *Artificial Intelligence and the Law*, Intersentia, Cambridge, 2021, pp. 359-403.
- DE LORENZO APARICI, O., «¿Pueden todas las aplicaciones de salud considerarse productos sanitarios?», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, pp. 87-109.
- DÍAZ ALABART, S., *Robots y responsabilidad civil*, Reus, Madrid, 2018.
- DÍAZ-REGAÑÓN GARCÍA-ALCALÁ, C., *Responsabilidad objetiva y nexo causal en el ámbito sanitario*, Comares, Granada, 2006.
- DÍEZ-PICAZO Y PONCE DE LEÓN, L., *Derecho de daños*, Civitas, Madrid, 1999.
- EBERS, M., «La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?», *InDret*, 3/2106, pp. 1-22.
- «¿Terapia sin terapeutas?: la interacción persona-robot en el marco del Reglamento sobre productos sanitarios de la UE y la Ley de Inteligencia Artificial», en *Servicios privados de telemedicina y salud digital: retos e implicaciones jurídicas*, dir. por R. Luquin Bergareche, Tirant lo Blanch, Valencia, 2023, pp. 77-158.
- EGUSQUIZA BALMASEDA, M.^a Á., «Pérdida de oportunidad por retraso diagnóstico. Algunas cuestiones desde la perspectiva jurisprudencial de la responsabilidad patrimonial», en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón*, coord. por Ataz López, J. y Cobacho Gómez, J. A., tomo II, Thomson Reuters Aranzadi, Cizur Menor (Navarra), pp. 255-282.
- EUROPEAN LAW INSTITUTE (ELI), *Draft of a Revised Product Liability Directive*, 2022, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf
- ELIZALDE SALAZAR, I., *Vehículos autónomos. Responsabilidad civil y seguro*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2022.
- ERCILLA GARCÍA, J., «Aproximación a una Personalidad Jurídica Específica para los robots», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 47, 2018, pp. 1-38.
- ESPINOSA FERNÁNDEZ, F., «Objeto, fundamento y naturaleza jurídica de la responsabilidad patrimonial de la Administración por asistencia sanitaria», en de Fuentes Bardají, Joaquín (director), *Manual sobre Responsabilidad Sanitaria*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2009, pp. 119-183.
- ESTER CASAS, V., «El concepto de la *lex artis* y su relevancia en la determinación de la relación de causalidad», en *Manual sobre Responsabilidad Sanitaria*, dir. por J. de Fuentes Bardají, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2009, pp. 219 y ss.
- EVANGELIO LLORCA, R., «A vueltas con la responsabilidad por daños derivados de servicios sanitarios al amparo del artículo 148 TRLGDCU», en *Cuestiones clásicas*

- y actuales del Derecho de daños. *Estudios en homenaje al Profesor Dr. Roca Guillamón*, Aranzadi, Cizur Menor (Navarra), 2021, pp. 475-532.
- «Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 549-620.
- FERRETTI, F., «Intelligenza Artificiale e responsabilità civile nel settore sanitario», *Actualidad Jurídica Iberoamericana*, núm. 18, febrero 2023, pp. 1852-1885.
- FRUTOS, Á., «Un robot realiza sin ayuda humana y con gran éxito la primera cirugía en tejido blando», *La Vanguardia*, 1 febrero 2022, <https://www.lavanguardia.com/tecnologia/20220201/8023051/robot-cirugia-sin-humanos-nbs.html>
- GALÁN CORTÉS, J. C., *Responsabilidad civil médica*, Civitas Thomson Reuters, 6ª ed., 2018.
- GALLARDO CASTILLO, M.^a J., *Administración sanitaria y responsabilidad patrimonial*, Colex, A Coruña, 2021.
- GARCÍA MICÓ, T. G., *Robótica quirúrgica y Derecho de daños*, Marcial Pons, Madrid, 2024.
- GARCÍA RUBIO, F. y FUENTES I GASÓ, J. R., *La responsabilidad de las Administraciones Públicas tras la nueva Ley de Régimen Jurídico del Sector Público*, Atelier, Barcelona, 2017.
- GIL MEMBRADO, C., *La responsabilidad civil por implante mamario. Mala praxis, consentimiento informado y prótesis defectuosa*, Comares, Granada, 2014.
- «Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el Derecho», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, pp. 357-399.
- «En el horizonte: la Directiva de responsabilidad extracontractual en materia de IA», en Gil Membrado, C. (dir. y coord.), *Derecho y medicina: desafíos tecnológicos y científicos*, Dykinson, Madrid, 2023, pp. 101-128.
- *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Reus, Madrid, 2023.
- GIL SALDAÑA, M., *El producto sanitario defectuoso en Derecho español*, Atelier, Barcelona, 2008.
- GOLDHILL, O., «Artificial intelligence can now predict suicide with remarkable accuracy», *Quartz*, June 10, 2017, <https://qz.com/1001968/artificial-intelligence-can-now-predict-suicide-with-remarkable-accuracy>
- GÓMEZ CALLE, E., «El fundamento de la responsabilidad civil en el ámbito médico-sanitario», *ADC*, vol. 51, núm. 4, 1998, pp. 1693-1767.
- GÓMEZ LIGÜERRE, C., «La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos», *Indret* 4.2022.

- GÓMEZ LIGÜERRE, C./GARCÍA MICÓ, T. G., «Liability for Artificial Intelligence and other emerging technologies», *Indret* 1.2020, pp. 501-511.
- GONZÁLEZ GONZÁLEZ, E., «Administración sanitaria y responsabilidad por productos sanitarios defectuosos con marchamo CE», *REDA*, n. 200/2019, pp. 1-29.
- GRIMALT SERVERA, P., «La responsabilidad (civil o patrimonial) del personal médico, de los centros sanitarios y de las administraciones sanitarias por los daños causados por un producto sanitario defectuoso», *Bioderecho.es*, núm. 17, enero-julio 2023, pp. 1-20.
- GUTIÉRREZ DE SANTIAGO, P., *Daños causados por productos defectuosos*, Thomson Aranzadi, Cizur Menor (Pamplona), 2008.
- HACKER, P., *Study about Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence. Complementary impact assessment*, European Parliamentary Research Service, Ex-Ante Impact Assessment Unit, September 2024 [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU\(2024\)762861_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf)
- HERBOSA MARTÍNEZ, I., «Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos», *Indret*, 3.2024, pp. 52-98.
- JORQUI AZOFRA, M., *Responsabilidad civil por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023.
- KARNER, E./KOCH, B. /GEISTFELD, M., *Comparative law study on civil liability for artificial intelligence*, estudio encargado por la Comisión Europea, Dirección General de Justicia y Consumidores, al *European Law Institute (ELI)*, Publications Office, Publications Office, 2021, disponible en: <https://data.europa.eu/doi/10.2838/66412>.
- KOCH, B., BORGHETTI, J. S., MACHNIKOWSKI, P., PICHONNAZ, P., RODRÍGUEZ DE LAS HERAS BALLELL, T., TWIGG-FLESNER, C., WENDEHORST, C., *Response of the European Law Institute (ELI) to the European Commission's Public Consultation on Civil Liability - Adapting Liability Rules to the Digital Age and Artificial Intelligence*, 2022 https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf
- LÓPEZ TUR, T., «Inteligencia artificial y responsabilidad civil en el ámbito sanitario», en *Derecho y salud: retos jurídicos actuales*, dir. por López Sánchez, C. y Ortiz Fernández, M., Aranzadi, Cizur Menor (Navarra), 2023, pp. 241-268.
- «Producto defectuoso e impresión de prótesis con impresoras 3D», en *Derecho y medicina: desafíos tecnológicos y científicos*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2023, pp. 45-68.
- LÓPEZ CANDELA, J. E., «El ámbito objetivo de la responsabilidad patrimonial de la Administración por funcionamiento normal con especial mención al servicio sanitario», *Revista Jurídica de Castilla y León*, núm. 15, mayo 2008, pp. 91-127.
- LUNA YERGA, Á., «Olvido de una gasa durante una intervención quirúrgica. Comentario a la STS, 1ª, 29.11.2002», *Indret*, 2.2003, pp. 1-14.

- LUQUIN BERGARECHE, R., «Responsabilidad contractual por el uso de la IA en la prestación de servicios de telemedicina y aplicaciones de salud digital», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 265-337.
- MARTÍN CASALS, M., «Desarrollo tecnológico y responsabilidad extracontractual: a propósito de los sistemas de Inteligencia Artificial (IA)», en Pérez Collados, J. M. (coord.), *La cultura jurídica en la era digital*, Aranzadi, Cizur Menor (Navarra), 2022, pp. 101-138.
- «La regulación de la responsabilidad extracontractual por daños causados por sistemas de Inteligencia Artificial (IA)», *RC-Revista de Responsabilidad Civil y Seguro*, año 60, núm. 1, enero 2023.
- MARTÍN CASALS, M. y SOLÉ FELIU, J., «¿Refundir o legislar? Algunos problemas de la regulación de la responsabilidad por productos y servicios defectuosos en el texto refundido de la LGDCU», *RDP*, septiembre-octubre 2008, pp. 79-111.
- MASCITTI, M., «La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos», *Revista de Derecho Privado*, núm. 42, 2022, pp. 215-260.
- MEDIAVILLA CABO, J. V., «Consideraciones sobre la responsabilidad de la administración pública sanitaria tras la crisis derivada del COVID 19», *Revista de Derecho vLex*, núm. 191, abril 2020, pp. 1-22.
- MOLLÁ, V., «IBM Watson al servicio de la medicina», 22 enero 2024, <https://www.victormolla.com/ibm-watson-medicina>
- MONJE BALMASEDA, Ó., «Robótica y responsabilidad en el ámbito sanitario», en *Bioderecho y retos. M-health, genética, IA, robótica y criogenización*, dir. y coord. por C. Gil Membrado, Dykinson, Madrid, 2022, pp. 429-456.
- MONTERROSO CASADO, E., «Responsabilidad civil por daños causados por robots en el ámbito sanitario», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y seguros*, dir. por Monterroso Casado, E. y coord. por Muñoz Villarreal, A., Tirant lo Blanch, Valencia, 2019, pp. 101-143.
- MORLA GONZÁLEZ, M., «Problemas jurídicos que plantean las terapias digitales para el rastreo del comportamiento del paciente», en *El Derecho y la justicia ante la inteligencia artificial y otras tecnologías disruptivas*, dir. por M. Castilla Barea y M.^a D. Cervilla Garzón, Aranzadi, Madrid, 2024, pp. 611-632.
- MUÑOZ VELA, J. M., *Retos, riesgos, responsabilidad y regulación de la inteligencia artificial*, Thomson Reuters Aranzadi, 2022.
- MUÑOZ VILLARREAL, A. y GALLEGU CORCHERO, V., «Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad de los robots», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y seguros*, dir. por Monterroso Casado, E. y coord. por Muñoz Villarreal, A., Tirant lo Blanch, Valencia, 2019, pp. 66-100.

- NAVARRO MENDIZÁBAL, I., «¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos», *Revista Iberoamericana de Bioética*, núm. 25, pp. 1-15.
- NAVARRO-MICHEL, «Vehículos automatizados y responsabilidad por producto defectuoso», *Revista de Derecho Civil*, vol. VII, núm. 5 (octubre-diciembre, 2020) pp. 175-223.
- NAVAS NAVARRO, S., «Responsabilidad civil del fabricante y tecnología inteligente», *la Ley*, núm. 35, sección Ciberderecho, 27.12.2019, pp. 1-11.
- *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022.
- «Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial», *Revista CESCO de Derecho de Consumo*, núm. 44/2022, pp. 27-51.
- NÚÑEZ ZORRILLA, M.^a C., «Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial», *Revista española de derecho europeo*, núm. 66, 2018, pp. 9-53.
- *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019.
- ORMAZABAL SÁNCHEZ, G., «La prueba en los procesos de responsabilidad civil por daños causados por sistemas de inteligencia artificial. Análisis del Derecho vigente y de las propuestas normativas de la UE», *InDret*, 3.2024, pp. 395-445.
- ORTIZ FERNÁNDEZ, M., *La responsabilidad civil derivada de los daños causados por sistemas inteligentes y su aseguramiento*, Dykinson, Madrid, 2021.
- PACHECO CAÑETE, M., «Reflexiones sobre la responsabilidad civil del empresario por los daños causados por sistemas de inteligencia artificial: situación actual y perspectivas futuras», *RGLJ*, 2023, núm. 2, pp. 281-317.
- PACHECO JIMÉNEZ, M.^a N., «Responsabilidad por daños desde la perspectiva del usuario de servicios sanitarios: del art. 28 LGDCU al art. 148 TRLGDCU», *Revista Jurídica sobre Consumidores y Usuarios*, núm. 4, enero 2019.
- PANIZA FULLANA, A., «La responsabilidad civil médico-sanitaria y la LGDCU», *Revista Doctrinal Aranzadi Civil-Mercantil*, 1998, pp. 1-49.
- PANTALEÓN PRIETO, F., «Cómo repensar la responsabilidad civil extracontractual (también la de las Administraciones Públicas)», en *Perfiles de la responsabilidad civil en el nuevo milenio*, coord. por J. A. Moreno Martínez, Dykinson, Madrid, 2000, pp. 439-468.
- PARRA LUCÁN, M.^a Á., *La protección del consumidor frente a los daños. Responsabilidad civil del fabricante y del prestador de servicios*, Reus, Madrid, 2011.
- «Responsabilidad civil por bienes o servicios defectuosos», en *Comentario del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias*, coord. por R. Bercovitz Rodríguez-Cano, 2^a ed., Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2015.

- PASQUAU LIAÑO, M., «El defecto de seguridad como criterio de imputación de responsabilidad al empresario de servicios», en *La responsabilidad civil por daños causados por servicios defectuosos*, dir. por A. Ortí Vallejo y M.^a del C. García Garnica, 2^a ed., Thomson-Aranzadi, Navarra, 2015, pp. 79-129.
- PEÑA LÓPEZ, F., «Comentario a la STS de 11 de febrero de 1998», *CCJC*, núm. 47, 1998, pp. 777-795.
- PERTÍÑEZ VÍLCHEZ, F., «Disposiciones comunes en materia de responsabilidad», en *La defensa de los consumidores y usuarios*, dir. por Rebollo Puig, M. e Izquierdo Carrasco, M., Iustel, Madrid, 2011, pp. 1811-1832.
- «Daños causados por otros bienes y servicios», en *La defensa de los consumidores y usuarios*, dir. por Rebollo Puig, M. e Izquierdo Carrasco, M., Iustel, Madrid, 2011, pp. 1905-1951.
- RACHUM-TWAIG, O., «Whose robot is it anyway?: Liability for artificial-intelligence-based robots», *2020 Univ. Ill. L.Rev.* 4, pp. 1141-1176.
- RAMÓN FERNÁNDEZ, F., «Inteligencia artificial en la relación médico-paciente: Algunas cuestiones y propuestas de mejora», *Revista Chilena de Derecho y Tecnología*, vol. 10, núm. 1, 2021, pp. 329-351.
- «El robot como producto defectuoso y responsabilidad civil», *Derecho Digital e Innovación*, núm. 14, 2022, pp. 1-28.
- REDACCIÓN APD, «Efectos de la inteligencia artificial en la medicina y sus aplicaciones más novedosas», 16 agosto 2024, <https://www.apd.es/aplicaciones-inteligencia-artificial-en-medicina/>
- RODRÍGUEZ DE LAS HERAS BALLELL, T., «La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzzle de la responsabilidad por daños causados por inteligencia artificial», *La Ley Mercantil*, núm. 103, Sección Derecho Digital, junio 2023, pp. 1-20.
- RODRÍGUEZ LÓPEZ, P., *Responsabilidad patrimonial de la administración en materia sanitaria*, Atelier, Barcelona, 2007.
- RUBÍ PUIG, A., «Retos de la inteligencia artificial y adaptabilidad del Derecho de Daños», en Cerrillo i Martínez, A./Peguera Poch, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2020.
- «Inteligencia artificial y daños indemnizables», en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, coord. por Álvarez Lata, N. (APPDC), Aranzadi, Madrid, 2024, pp. 621-688.
- RUIZ JIMÉNEZ, J., «La aplicación de responsabilidad objetiva en los servicios sanitarios», *RCDI*, núm. 700, marzo-abril 2007, pp. 847-852.
- SALVADOR CODERCH, P. Y OTROS, «Los riesgos del desarrollo», *InDret* 1/2001, pp. 1-30.
- SÁNCHEZ CAJA, A., «La aplicación de la IA en los hospitales puede reducir hasta un 50% el coste de la atención al paciente», *EDS Revista Española de Economía de*

- la Salud*, 16 febrero 2024, <https://eonomiadelasalud.com/topics/difusion/la-aplicacion-de-la-ia-en-los-hospitales-puede-reducir-hasta-un-50-el-coste-de-la-atencion-al-paciente/>
- SÁNCHEZ DEL CAMPO REDONET, A., *Reflexiones de un replicante legal. Los retos jurídicos de la robótica y las tecnologías disruptivas*, Aranzadi, Cizur Menor (Navarra), 2016.
- SANTOS MORÓN, M.^a J., «La imputación de responsabilidad médica con base en las normas de protección de consumidores: el artículo 148 TRLC», *ADC*, tomo LXX, 2017, fasc. 1, pp. 119-164.
- SOLÉ FELIU, J., «Estándar de diligencia médica y valor de los protocolos y guías de práctica clínica en la responsabilidad civil de los profesionales sanitarios», *Revista de Derecho Civil*, vol. IX, núm. 3 (julio-septiembre, 2022), pp. 1-52.
- STRICKLAND, E., «AI Predicts Heart Attacks and Strokes More Accurately Than Standard Doctor's Method», *IEEE Spectrum*, 01 May 2017, <https://spectrum.ieee.org/ai-predicts-heart-attacks-more-accurately-than-standard-doctor-method>
- TOLOSATRIBIÑO, C., «La responsabilidad patrimonial de la Administración», *Abogacía española. Consejo General*, 14 marzo 2024, <https://www.abogacia.es/actualidad/opinion-y-analisis/la-responsabilidad-patrimonial-de-la-administracion/>
- ZURITA MARTÍN, I., *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020.
- «Las propuestas de reforma legislativa del Libro Blanco Europeo sobre Inteligencia Artificial en materia de seguridad y responsabilidad civil», *Actualidad Jurídica Iberoamericana*, n. 14, febrero 2021, pp. 438-487.

Los *deepfakes* y la intromisión en los derechos de la personalidad (imagen, voz, honor y protección de datos) y sus mecanismos de reparación¹

BEATRIZ EXTREMERA FERNÁNDEZ

*Profesora Ayudante Doctora de Derecho civil.
Universidad de Alicante*

Sumario: 1. INTRODUCCIÓN. 2. PRECISIONES CONCEPTUALES: QUÉ ES EL *DEEPPFAKE* Y SU CLASIFICACIÓN DEL RIESGO. 3. PROBLEMÁTICA JURÍDICA DEL *DEEPPFAKE*. **3.1. Los derechos al honor, a la propia imagen y a la voz en la LO 1/1982.** 3.1.1. *La confrontación con el derecho a la propia imagen y a la voz.* 3.1.2. *La confrontación con el derecho al honor.* 3.1.3. *Exclusión de la ilegitimidad de la injerencia de estos derechos.* A) El consentimiento del uso del *deepfake*. B) Las intromisiones autorizadas por Ley. 3.1.4. *La utilización del deepfake post mortem.* **3.2. La imagen y voz como datos de carácter personal en el uso del deepfake.** 4. EL PAPEL DE LA ADVERTENCIA EN EL USO DEL *DEEPPFAKE*. 5. MECANISMOS DE PROTECCIÓN. **5.1. La tutela de los derechos de la personalidad protegidos en la LO 1/1982.** **5.2. La tutela de los datos de carácter personal.** **5.3. La responsabilidad de los prestadores de servicios de la sociedad digital.** 6. CONCLUSIONES. 7. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

No cabe duda de que la Inteligencia Artificial ha supuesto grandes retos para la sociedad actual. Retos a los que, poco a poco, el legislador -sobre

¹ Trabajo realizado al amparo de los Proyectos «La irrupción de la inteligencia artificial en el Derecho de daños y su adaptación a las nuevas tecnologías» - Referencia PID2020-116185GB-I00 (Ministerio de Ciencia e Innovación - Agencia Estatal de investigación) y «La Unión Europea ante los desafíos regulatorios de la Inteligencia Artificial: cuestiones de responsabilidad civil» - CIGE/2023/196 (Conselleria d'Educació, Cultura, Universitats i Ocupació de la Generalitat Valenciana)».

todo el europeo- ha querido ir adaptando a la realidad jurídica. En efecto, hace unos años la creación de contenidos con Inteligencia Artificial estaba, únicamente, al alcance de las grandes producciones de Hollywood, por ejemplo, para la finalización de un largometraje durante la producción del cual un actor había fallecido, tal y como sucedió con la aparición en 2015 de Paul Walker en la película *Fast & Furious 7* tras su fallecimiento. Sin embargo, poco a poco estas creaciones con Inteligencia Artificial se fueron haciendo más populares e incluso se utilizó la voz e imagen de la fallecida Lola Flores para la promoción de la cerveza Cruzcampo en su anuncio «Con acento» y de Luis Aragonés para un anuncio de LaLiga, también tras su defunción. Finalmente, hoy en día el uso de esta tecnología se encuentra al alcance de cualquier usuario que tenga nociones medias de informática e, incluso, hay programas gratuitos y aplicaciones sencillas que hacen esta tecnología todavía más accesible.

Esta tecnología, denominada «ultrasuplantaciones» o «ultrafalsificaciones», aunque popularmente es conocida como *deepfake* (por la combinación de las palabras inglesas *deep learning* y *false*, esto es, «aprendizaje profundo» y «falsificación», respectivamente), se refiere a la creación de imagen, video o sonido falsos, pero que tienen la apariencia de ser reales. Si bien es cierto que las ultrafalsificaciones pueden ser muy útiles en los campos de la educación, comunicación digital, así como en la industria de los videojuegos, moda o comercio electrónico², también pueden suponer nuevos riesgos que conviene abordar.

En efecto, los *deepfakes* se han utilizado para la creación de videos o de imágenes de políticos que pueden influir en las tendencias políticas, siendo los más populares las ultrafalsificaciones creadas a partir de la imagen y voz de Barack Obama y de Donald Trump, o para crear campañas de desinformación³; asimismo, para la creación de canciones a partir de la voz de famosos cantantes (incluso, en ocasiones, estas canciones se han escrito utilizando Inteligencia Artificial, en concreto, ChatGPT)⁴; y, finalmente, el uso de las ultrasuplantaciones más controvertido ha sido la creación de contenido por-

² Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Review* (9), 41.

³ Sobre los riesgos de la desinformación, Gómez de Ágreda, Á., Feijóo, C., Salazar García, I. A. (2021). Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital. Deep fakes e inteligencia artificial. *Profesional de la información*, (30, 2).1-24; García Ull, F. (2021). Deepfakes: el próximo reto en la detección de noticias falsas. *Anàlisi: Quaderns de Comunicació i Cultura* (64), 103-120.

⁴ Son muchos los cantantes que han sufrido de la creación de canciones a partir de la citada tecnología con la utilización de sus voces (por ejemplo, Taylor Swift, Beyoncé, Drake, The Weekend, Eminem y, en lo que al panorama hispanohablante se refiere, destacan los cantantes de música urbana Bad Bunny, Bad Gyal o Eladio Carrión) y muchos de ellos se han quejado de la desprotección que existe a este respecto.

nográfico a partir de la imagen de personajes famosos o, incluso, de menores de edad⁵.

Todo ello, sin lugar a duda, supone una intromisión en los derechos de la personalidad y, por ello, es necesario un análisis pormenorizado de la problemática jurídica que se plantea, así como de la protección que pueden exigir los particulares ante el uso de las ultrasuplantaciones. Ahora bien, la existencia de estos riesgos no puede suponer la prohibición del uso de la citada tecnología, sino que lo que se debe pretender es el establecimiento de ciertos límites con el fin de que pueda ser utilizada sin que ello suponga un grave riesgo. Ante esta disyuntiva, el presente estudio pretende analizar la confrontación del uso del *deepfake* con aquellos derechos de la personalidad a los que el uso del mismo puede suponer una problemática jurídica mayor, en concreto, el derecho a la propia imagen, voz, honor y a la protección de datos.

2. PRECISIONES CONCEPTUALES: QUÉ ES EL *DEEPPFAKE* Y SU CLASIFICACIÓN DEL RIESGO

Antes de iniciar con el estudio de las implicaciones jurídicas de las ultrafalsificaciones conviene precisar a qué nos referimos cuando hablamos de este tipo de tecnología.

El *deepfake* se basa en las Redes Generativas Adversativas (GAN, por sus siglas en inglés), esto es, en dos redes neuronales artificiales que trabajan de manera conjunta para crear imágenes, videos o sonidos de apariencia real. En este sentido, una red neuronal (generadora) crea nuevos medios a partir de imágenes, videos o sonidos que pretenden convencer a la segunda red neuronal (discriminadora) de que estas son reales. Por su parte, la discriminadora debe detectar que dichos medios no lo son. De este modo, ambas redes neuronales trabajan conjuntamente para aprender la una de la otra y perfeccionar la técnica de ambas. Ahora bien, aunque en un principio los *deepfakes* requerían de una amplia base de datos para crear una falsificación realista,

⁵ Tal y como destaca Simó Soler, E. (2023) Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho. *InDret. Revista para el análisis del Derecho* (2), 5, el 96% de los *deepfakes* disponibles en internet se trata de contenido sexual sin consentimiento, el 99% de los cuales las víctimas son mujeres. Téngase presente que la creación de contenido pornográfico no se encuentra tipificado en el artículo 197 del Código Penal, en tanto que el contenido creado, por definición, es falso y, por ende, no supone una revelación de secretos. La misma autora considera que sería necesario para penalización de esta conducta la creación de una subcategoría subsumible en el tipo del artículo 197 del Código Penal. Simó Soler, 2023: 14.

esta tecnología se ha desarrollado hasta el punto de utilizar únicamente una imagen, video o sonido para crear una falsificación realista⁶.

Desde el punto de vista jurídico, encontramos una reciente descripción en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), que define en su artículo 3.60) la «ultrasuplantación» como «un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares u otras entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos»⁷.

Esta tecnología, además de tener beneficios en las diferentes industrias como se ha advertido previamente, también puede presentar riesgos para los derechos de la personalidad de los particulares. De este modo, si atendemos a la clasificación del riesgo que hace el Reglamento de Inteligencia Artificial, no consideramos que la tecnología *deepfake* se encuentre entre los sistemas de alto riesgo definidos en el artículo 6 del citado texto normativo. En efecto, debe descartar que se trate de un sistema de alto riesgo al no ser una de las tecnologías citadas en el primer apartado del artículo 6, ni tampoco una de las citadas en el Anexo III del Reglamento de Inteligencia Artificial. Sin embargo, tampoco podemos considerar que se trate de un sistema de mínimo o de no riesgo, dado que el propio Reglamento establece ciertas obligaciones de transparencia. En definitiva, nos encontramos ante un sistema de Inteligencia Artificial con específicas obligaciones de transparencia, por cuanto que el artículo 50.4 del Reglamento de Inteligencia Artificial exige que «Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial [...]». Ahora bien, este mismo precepto exime dicha obligación cuando esta técnica «forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción», en cuyo caso únicamente se exige que se advierta de la existencia de contenido generado o manipulado

⁶ Westerlund, 2019: 40-41.

⁷ Hasta la Resolución del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, el texto legislativo en castellano utilizaba el término «ultrafalsificación». Sin embargo, en el texto definitivo y su publicación en esta lengua, se ha optado por la utilización del término «ultrasuplantación».

artificialmente, pero de manera que no dificulte la exhibición o el disfrute de la obra (por ejemplo, con una advertencia inicial o final).

Este deber de transparencia ya estaba contemplado en el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) en su artículo 35.1.k): «Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda de muy gran tamaño aplicarán medidas de reducción de riesgos razonables, proporcionadas y efectivas, adaptadas a los riesgos sistémicos específicos detectados de conformidad con el artículo 34, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos fundamentales. Dichas medidas podrán incluir, cuando proceda: [...] k) garantizar que un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información»⁸.

Así pues, el tratamiento que se ha dado de las ultrasuplantaciones por parte de la normativa europea es que se trata de un sistema de riesgo sometido a deberes de transparencia. Sin embargo, a nuestro juicio, esta consideración resulta insuficiente. Por un lado, se trata la problemática generada por el *deepfake* como si el único riesgo existente mediante el uso de esta tecnología fuera la desinformación. Sin embargo, su riesgo va más allá, en tanto que, como se analizará a continuación, el uso de esta puede atentar contra derechos de la personalidad. En este sentido, Gutiérrez García considera que debería haberse clasificado las ultrasuplantaciones como un riesgo alto enunciado en el Anexo III del Reglamento de Inteligencia Artificial, por cuanto que el Considerando 7 del citado texto enuncia que la clasificación de los sistemas de Inteligencia Artificial de alto riesgo se realiza para «garantizar un nivel elevado y coherente de protección de los intereses públicos en lo que respecta a la salud, la seguridad y los derechos fundamentales [...]»⁹.

Por el otro lado, las obligaciones de transparencia que trata el Reglamento de Servicios Digitales solo se contemplan para «plataformas en línea de muy

⁸ A este respecto, las aplicaciones de la compañía «META» permiten que los usuarios adviertan que se ha utilizado Inteligencia Artificial Generativa para la creación de una publicación, como podría ser, por ejemplo, el uso de *deepfake*.

⁹ Gutiérrez García, E. (2024). *Daños ocasionados por sistemas de Inteligencia Artificial*. Comares. 180-181.

gran tamaño y motores de búsqueda en línea de *muy gran tamaño*¹⁰. De este modo, se ha criticado que las obligaciones impuestas deberían ser más exigentes y, además, debería ser requeridas a cualquier plataforma en línea y no solamente a las de *muy gran tamaño*¹¹. Por su parte, en el Reglamento de Inteligencia Artificial esta exigencia no es de las plataformas en línea, sino que es de los responsables del despliegue de los sistemas de Inteligencia Artificial, entendiendo por estos: «una persona física o jurídica, o autoridad pública, órgano u organismo, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue» (art. 3.4 y Considerando 13 del Reglamento de Inteligencia Artificial). A nuestro juicio, esto sigue siendo insuficiente, en tanto que el deber de transparencia debería ser extendido a cualquier persona que genere una ultrasuplantación que pueda afectar a los derechos de la personalidad, dado que los particulares que no tienen ningún fin profesional también pueden conculcar derechos de la personalidad.

En cuanto al sistema jurídico español, basta decir que no contamos con previsiones a tal efecto, pero existen dos proposiciones de leyes orgánicas que sí que han visto el potencial de la conculcación de los derechos fundamentales de las ultrafalsificaciones. Por un lado, cabe mencionar la Proposición de Ley Orgánica de refuerzo de las medidas para restringir el acceso de los menores de dieciséis años a la pornografía¹², que pretende, entre otras modificaciones, incorporar un apartado 8 al artículo 197¹³ que tipifique la creación de *deepfakes* cuando la divulgación de dicho contenido menoscabe el honor o la intimidad¹⁴.

¹⁰ La cursiva es nuestra.

¹¹ Gutiérrez García, 2024: 152-153.

¹² Proposición de Ley Orgánica de refuerzo de las medidas para restringir el acceso de los menores de dieciséis años a la pornografía (122/000326), presentada por el Grupo Parlamentario Plural. BOCG de 19 de mayo de 2023, núm. 353-1.

¹³ «El que utilice imágenes de gran verosimilitud (“deepfake”) elaboradas con inteligencia artificial para reproducir la imagen de una persona o utilice imágenes reales obtenidas sin su consentimiento con el objetivo de crear contenidos audiovisuales que puedan ser difundidos públicamente por cualquier medio, cuando la divulgación menoscabe gravemente el honor o la intimidad de esa persona, será castigado con pena de seis meses a dos años.

Se impondrá la pena de multa de uno a tres meses a quien, habiendo recibido las imágenes o grabaciones audiovisuales a las que se refieren los párrafos 7 y 8 las difunda, revele o ceda a terceros son el consentimiento de la persona afectada.

En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa».

¹⁴ Tal y como destaca Simó Soler, E. (2023) Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho. InDret.

Por el otro lado, destaca la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de inteligencia artificial¹⁵ que, entre otras proposiciones, pretende la tipificación de la creación de ultrasuplantaciones que, sin contar con el consentimiento de la persona afectada, menoscaben su honor, fama, dignidad o propia estimación¹⁶. Asimismo, incorpora un apartado noveno al artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante, LO 1/1982), que considera el uso de las ultrafalsificaciones una intromisión legítima, salvo que exista una advertencia sobre el carácter de su origen falso¹⁷. Y, además, la presente Proposición también quiere incorporar un artículo 22 bis a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD) que reconozca la aplicación de dicha ley a la generación de *deepfakes*¹⁸.

Revista para el análisis del Derecho (2), 5, el 96% de los deepfakes disponibles en internet se trata de contenido sexual sin consentimiento, el 99% de los cuales las víctimas son mujeres. Téngase presente que la creación de contenido pornográfico no se encuentra tipificado en el artículo 197 del Código Penal, en tanto que el contenido creado, por definición, es falso y, por ende, no supone una revelación de secretos. La misma autora considera que sería necesario para penalización de esta conducta la creación de una subcategoría subsumible en el tipo del artículo 197 del Código Penal. Simó Soler, 2023: 14.

¹⁵ Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial (122/000011), presentada por el Grupo Parlamentario Plurinacional SUMAR. BOCG 13 de octubre de 2023, núm. 23-1.

¹⁶ «Artículo 208 bis. Igualmente tendrá la consideración de injuria la acción que, sin autorización y con ánimo de menoscabar el honor, fama dignidad o la propia estimación de una persona, recrease mediante sistemas automatizados, software, algoritmos o inteligencia artificial para la pública difusión su imagen corporal o audio de voz».

«Artículo 211. La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Salvo previa autorización expresa de la persona o personas afectadas, las simulaciones de imágenes, vídeos o audios de voz de estas generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial que fueran difundidos a través de redes sociales serán consideradas como injurias hechas con publicidad».

¹⁷ «La difusión y utilización de imágenes y vídeos de personas o audios de voz generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial sin la previa autorización o consentimiento expreso de la persona o personas afectadas, excepto que incluyan de [] forma clara y sobresaliente una advertencia de su condición de imagen o audio de voz generado artificialmente por inteligencia artificial. La advertencia deberá figurar sobreimpresa y legible en la propia imagen. Para el caso de los audios de voz deberá realizarse una advertencia audible antes y después de su difusión».

¹⁸ «Artículo 22 bis. Tratamiento de datos generados por inteligencia artificial. La presente ley se aplicará a los datos personales generados con imágenes, audios o sonido utilizados por el algoritmo para realizar el aprendizaje automático necesario para generar patrones, imágenes o sonidos de inteligencia artificial que sean difundidos públicamente».

3. PROBLEMÁTICA JURÍDICA DEL *DEEPFAKE*

Sin perjuicio de lo anteriormente expuesto, esto es, de la clasificación de las ultrasuplantaciones como un sistema de Inteligencia Artificial sometido a obligaciones de transparencia, pero no como un sistema de alto riesgo, no debe llegar a pensarse que esta técnica no cuenta con grandes riesgos, por el contrario, el uso de esta tecnología ha planteado grandes problemáticas jurídicas. Así es, el uso de las ultrafalsificaciones puede conllevar graves riesgos para los derechos de la personalidad, como lo son el derecho al honor, a la propia imagen y a la voz, así como a la protección de datos. Sin embargo, esto no puede suponer una prohibición radical de los *deepfakes*, dado que su uso también puede venir justificado al amparo de la libertad de expresión, por ejemplo, es por ello por lo que resulta necesario un análisis de la problemática jurídica surgida al amparo de esta tecnología con el objetivo de ponderar los derechos implicados.

3.1. LOS DERECHOS AL HONOR, A LA PROPIA IMAGEN Y A LA VOZ EN LA LO 1/1982

Si bien es cierto que la LO 1/1982 protege distintos derechos de la personalidad, no todos son relevantes en lo que a la aplicación de *deepfake* se refiere. Y es que, en principio, las ultrafalsificaciones afectan, sobre todo, al derecho de la propia imagen, voz y honor; mientras que otros derechos no se ven apenas afectados por el uso de la citada tecnología, como puede ser el de la intimidad personal y familiar, en tanto que el uso de esta no supondría un nuevo reto a estos últimos derechos¹⁹. Es por ello por lo que en el presente apartado nos centraremos en los derechos a la propia imagen, voz y honor.

3.1.1. La confrontación con el derecho a la propia imagen y a la voz

Los primeros derechos de la personalidad que pueden interferir en el uso de la tecnología *deepfake* son el derecho a la propia imagen y a la voz, en tanto que las ultrafalsificaciones utilizan la imagen y la voz de una persona concreta para simular que esta hace o dice algo que, en realidad, no ha hecho o dicho.

¹⁹ Consideramos que no afecta al derecho de la intimidad (a diferencia de lo indicado en la Proposición de Ley Orgánica de refuerzo de las medidas para restringir el acceso de los menores de dieciséis años a la pornografía) por cuanto que las imagen generadas con esta tecnología que podrían parecer atentar contra el derecho a la intimidad (la creación de imágenes pornográficas, por ejemplo), en realidad, son falsas y, por ende, no atentan contra la intimidad del afectado, sino contra su derecho a la propia imagen o el honor o, incluso, contra la protección de los datos personales.

En primer lugar, el derecho a la imagen se refiere a la protección de los rasgos físicos personales²⁰. De este modo, puede concluirse que la protección de este derecho no se refiere a la «imagen social» de una persona y que, además, no se limita a las situaciones desfavorables o que atenten contra la estima o aspectos privados de su vida. Así es, el derecho a la imagen tiene una protección autónoma del resto de derechos que protege el artículo 18.1 CE y, por tanto, la tutela de este no se limita a las injerencias en el derecho al honor o a la intimidad de la persona, sino que nos encontramos ante un derecho plenamente autónomo²¹.

En cuanto al contenido de este, se permite, por un lado, que la persona titular del derecho consienta la captación, reproducción o publicación de su imagen y, por el otro, que este mismo puede impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad de quien la persigue o de quien la capta²². Además, se protege el contenido de este derecho con independencia del medio o la técnica mediante la que se capture, reproduzca o publique la imagen del titular, esto es, no importa que la imagen se capte mediante fotografía o video o mediante la representación de la misma a través de la pintura o de la

²⁰ De Verda y Beamonte, J. R. (2007a). El derecho a la propia imagen. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 145-179). Aranzadi. 149.

²¹ Así se desprende de la STC núm. 81/2001, de 26 de marzo, FJ 2 [RTC 2001\81]: «La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad [...] No cabe desconocer que mediante la captación y publicación de la imagen de una persona puede vulnerarse tanto su derecho al honor como su derecho a la intimidad. Sin embargo, lo específico del derecho a la propia imagen es la protección frente a las reproducciones de las misma que, afectando a la esfera personal de su titular, no lesionan su buen nombre ni dan a conocer su vida íntima. El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás». Asimismo, la STC núm. 156/2001, de 2 de julio, FJ 3 [RTC 2001\156]: «puede vulnerarse el derecho a la propia imagen sin conculcar el derecho a la intimidad, supuesto éste que se producirá cuando las imágenes permitan la identificación de la persona fotografiada, pero no entrañen una intromisión en su intimidad».

Asimismo, De Verda y Beamonte, 2007a: 149-150; Navas Sánchez, M. M. (2017). El derecho a la propia imagen de los personajes públicos en las jurisprudencias constitucional, ordinaria y europea. Evolución concordancias y divergencias. *Revista de Derecho Político* (100), 444; Trujillo Cabrera, C. (2024). El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial. *InDret. Revista para el análisis del Derecho* (1), 86.

²² De Verda y Beamonte, 2007a: p. 149; De Verda y Beamonte, J. R. y De las Heras Vives, L. (2019). Los derechos de la personalidad frente al sexting, streaming y otros fenómenos digitales: nuevos retos para su estudio, vigencia y protección en el siglo XXI. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 181-228). Tirant lo Blanch; Ysás Solanes, M. (2013). Derechos en la esfera moral. En M. C. Gete-Alonso y Calera (Dir.) y J. Solé Resina (Coord.), *Tratado de derecho de la persona física. Tomo II* (pp. 833-876). Civitas-Aranzadi. 843.

escultura, dado que, en todos los casos, el titular del derecho podrá negarse a su captación o reproducción²³.

Por su parte, definir el «derecho» a la propia voz es más complejo por diversos motivos: por un lado, por el escaso tratamiento dado por la jurisprudencia constitucional y la doctrina a este respecto; por el otro lado, porque cuando se ha abordado, se debate entre la autonomía del derecho a la voz frente a otros derechos de la personalidad y su reconocimiento como un aspecto más del derecho de la intimidad, del honor o, sobre todo, de la propia imagen.

En relación con la postura de la jurisprudencia constitucional, el Tribunal Constitucional no ha reconocido la autonomía del derecho a la voz frente al resto de derechos de la personalidad del artículo 18.1 CE. Ahora bien, la posición mantenida al respecto por el citado tribunal es errática por cuanto que lo ha situado como una manifestación de diferentes derechos de la personalidad. En un primer momento lo situó como una manifestación del derecho a la intimidad (STC 114/1984, de 29 de noviembre²⁴) y, posteriormente, lo situó en la esfera del derecho a la propia imagen (STC 117/1994, de 25 de abril²⁵). Sin embargo, con posterioridad, el Tribunal Constitucional se refirió al derecho a la imagen como el «derecho a determinar la información gráfica generada por los rasgos físicos personales de su titular que puede tener difusión pública» (STC 23/2010, de 27 de abril²⁶), por tanto, la voz no queda amparada en el derecho a la propia imagen por cuanto que no atiende a la definición propuesta por el citado Tribunal.

Por lo que al posicionamiento doctrinal se refiere, la doctrina mayoritaria ha considerado que nos encontramos ante un derecho de la personalidad autónomo del resto y que, por ende, puede ser objeto de protección autónoma²⁷.

²³ Trujillo Cabrera, 2024: 86.

²⁴ STC núm. 114/1984, de 29 de noviembre, FJ 8 [RTC 1984\114]: «Tal protección de la propia voz existe sólo en el Derecho español, como concreción del derecho a la intimidad y, por ello mismo, sólo en la medida en que la voz ajena sea utilizada “ad extra” y no meramente registrada, y aun en este caso cuando dicha utilización lo sea con determinada finalidad».

²⁵ STC núm. 117/1994, de 25 de abril, FJ 3 [RTC 1994\117]: «En la medida en que la libertad de ésta se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz».

²⁶ STC núm. 23/2010, de 27 de abril, FJ 4 [RTC 2010\23]. Asimismo, las SSTC núm. 81/2001, de 26 de marzo, FJ 2 [RTC 2001\81]; núm. 139/2001, de 18 de junio, FJ 4 [RTC 2001\139]; núm. 83/2002, de 22 de abril, FJ 4 [RTC 2002\83]; núm. 14/2003, de 28 de enero, FJ 5 [RTC 2003\14]; núm. 19/2014, de 10 de febrero, FJ 5 [RTC 2014\19].

²⁷ De Verda y Beamonte, 2007a: 163; De Verda y Beamonte, J. R. (2007c). Las intromisiones en los derechos al honor, intimidad y propia imagen autorizadas por la Ley. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección*

Los argumentos esgrimidos para fundamentar la citada conclusión son muchos y variados: en primer lugar, el tenor literal del artículo 7.6º de la LO 1/1982 reconoce que: «Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley: [...] 6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga»²⁸; en segundo lugar, si se considera que el anterior argumento esgrimido no fuera suficiente, debe recordarse que la enumeración de las intromisiones ilegítimas que realiza el artículo 7 de la LO 1/1982 es abierta, es decir, se trata de un *numerus apertus*²⁹; en tercer lugar, el artículo 10.1 de la Constitución Española («La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social») sirve de base para la creación de nuevos derechos y, entre ellos, puede estar el derecho a la voz³⁰; finalmente, otro argumento que justifica dicha autonomía es que si se permite el uso inocuo de la voz puede ocasionar problemas jurídicos, aun cuando ello no afecte a otros derechos de la personalidad tradicionales³¹.

Por el contrario, Gutiérrez García considera que el bien jurídico protegido del derecho a la propia imagen se compone, además de los rasgos físicos, del nombre y la voz de la persona, y ello en atención a la interpretación sistemática del artículo 7.6 de la LO 1/1982³².

Sin perjuicio de lo anteriormente expuesto, cabe afirmar que la voz debe estar protegida, ya sea como un aspecto más del derecho a la propia imagen, ya sea mediante una protección autónoma. Así las cosas, se puede definir el ámbito de protección del bien jurídico protegido de la voz como aquel que permite al titular la facultad de oponerse a la reproducción de su voz, por ser esta un atributo de su personalidad. Asimismo, también puede impedir

Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen (pp. 255-277). Aranzadi. 276; Roselló Manzano, R. (2011). *Derechos de la personalidad y derechos morales de los autores*. Editorial Reus. 65. De Verda y Beamonte, J. R. (2017). Los derechos fundamentales de la personalidad (al honor, a la intimidad y a la propia imagen) como categoría unitaria. *Revista Boliviana de Derecho* (23), 103; Ammerman Yebra, J. (2021). *El derecho a la propia voz como derecho de la personalidad*, Colex. 237; Trujillo Cabrera, 2024: p. 90.

²⁸ De Verda y Beamonte, 2007a: 163; De Verda y Beamonte, 2007c: 276; Ammerman Yebra, 2021: 237.

²⁹ Ammerman Yebra, 2021: 237. Aunque no se refiere al derecho a la voz, también defiende que el artículo 7 se trata de una enumeración abierta Ysás Solanes (2013: 853).

³⁰ García Rubio, M. P. (2013). Los derechos de la personalidad. En M. C. Gete-Alonso y Calera (Dir.) y J. Solé Resina (Coord.), *Tratado de derecho de la persona física. Tomo II* (pp. 597-631). Civitas-Aranzadi. 610-612; Ammerman Yebra, 2021: 237.

³¹ Trujillo Cabrera, 2024: 90.

³² Gutiérrez García, 2024: 159.

aquellas imitaciones que puedan ocasionar una confusión con el titular del derecho³³.

Tras el análisis de estos derechos desde un punto de vista tradicional, conviene cuestionarse cómo les afecta el uso de la tecnología *deepfake*. Y es que debe reconocerse que el contenido generado por esta técnica de Inteligencia Artificial no es real y, por ende, podría pensarse que no supone injerencia alguna a los derechos a la propia imagen y a la voz del titular de los derechos por ser estos una simulación. Sin embargo, no cabe duda de que las ultraplantaciones pueden suponer una intromisión en los derechos analizados en tanto que, si bien es cierto que se trata de recreaciones ficticias, estas son tan buenas que las personas titulares de estos derechos son perfectamente reconocibles e, incluso, en muchas ocasiones, lo que se pretende es causar esa confusión.

En cuanto al uso de la tecnología, es necesario diferenciar dos momentos distintos: el primero, cuando son utilizados la imagen o la voz original de la persona afectada para el entrenamiento de la red neuronal; el segundo momento, cuando la red neuronal recrea la imagen o la voz de la persona titular de los derechos³⁴. De este modo, ambos momentos deben contar con alguna de las causas de legitimación a las que se refiere la LO 1/1982 o ha de haberse prestado el consentimiento del afectado para que se haga uso de su imagen y de su voz mediante esta tecnología. En efecto, debe recordarse que el derecho a la propia imagen incluye en su tutela cualquier representación que se haga de la imagen, ya sea esta realizada mediante una fotografía, un video, una escultura, pintura o caricatura o mediante cualquier otro procedimiento³⁵, entre los que debemos incluir, en este caso, el uso del *deepfake*. Lo mismo sucede con el derecho a la voz, como ya se ha comentado anteriormente, el titular del derecho puede impedir aquellas imitaciones que puedan ocasionar una confusión y, sin lugar a duda, las creaciones de *deepfake* podrían encuadrarse en esta situación. A partir de tales premisas, resulta necesario analizar en qué situaciones se justifica y legitima las injerencias a estos derechos. A tales efectos, se analizarán las causas tradicionales de legitimación del uso de la imagen y la voz para ponerse en relación con su aplicación en el *deepfake*.

³³ De Verda y Beamonte, 2007a: 165; De Verda y Beamonte, 2007c: 276; Roselló Manzano, 2011: 64-65. De Verda y Beamonte, 2017: 103.

³⁴ Vega García, P. (2023). Protección y comercialización del derecho a la propia imagen del difunto ante la inteligencia artificial. En A. Arrébola Blanco (Dir.), *Retos del Derecho de sucesiones en el siglo XXI. Vol. II* (pp. 999-1024). Reus. 1019-1020.

³⁵ Trujillo Cabrera, 2024: 86.

3.1.2. La confrontación con el derecho al honor

Otro de los derechos de la personalidad a análisis al que puede afectar el uso de *deepfake* es el derecho al honor, en tanto que esta tecnología puede crear un contenido falso en el que parezca que una persona hace o dice algo que, en realidad, no ha hecho o ha dicho, pero que afecte a su honor.

El derecho al honor, en el ámbito internacional, se enmarca dentro del derecho a la privacidad en el artículo 12 de la Declaración Universal de Derechos Humanos («Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación [...]»), en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea («Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones»), el artículo 17.1 del Pacto Internacional de Derechos civiles y Políticos («Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación») y el artículo 8 del Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales («Toda persona tiene derechos al respeto de su vida privada y familiar, de su domicilio y de su correspondencia»). Por lo que al Derecho español se refiere, el derecho al honor se reconoce en el artículo 18.1 CE y se desarrolla en la citada LO 1/1982.

La definición del derecho al honor es compleja por cuanto que la propia concepción del honor dependerá del momento histórico, normas, valores e ideas sociales vigentes en cada momento³⁶, así el Tribunal Constitucional lo ha considerado como «lábil y fluido y cambiante»³⁷. En este sentido, este derecho protege «la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que le hagan desmerecer en la consideración ajena al ir en su descrédito o menosprecio o que sean tenidas en el concepto público por afrentosas»³⁸.

De este modo, se puede constatar la prevalencia del criterio objetivo, esto es, la reputación que socialmente tiene una persona, frente al criterio subje-

³⁶ STC núm. 180/1999, de 11 de octubre, FJ 4 [RTC 1999\180]. En este mismo sentido, Moliner Navarro, R. (2007a). El derecho al honor y su conflicto con la libertad de expresión y el derecho a la información. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 21-53). Aranzadi. 24-26.

³⁷ STC núm. 170/1994, de 7 de junio, FJ 4 [RTC 1994\170].

³⁸ STC núm. 180/1999, de 11 de octubre, FJ 4 [RTC 1999\180]. En un sentido similar, la STC núm. 52/2002, de 25 de febrero, FJ 4 [RTC 2002\52].

tivo, es decir, el daño moral que se produce en la propia estima de la persona ante las afirmaciones que se acometen contra de ella³⁹.

Basta decir que la conculcación del derecho al honor puede realizarse a través de manifestaciones escritas u orales o, también, a través de la divulgación de la imagen en un contexto que suponga un descrédito de la persona titular del derecho⁴⁰.

Sin embargo, este derecho, como el resto, no es absoluto y debe ser ponderado con el derecho a la información y a la libertad de expresión. En cuanto al primero, no parece que pueda ser aplicable en tanto que el *deepfake* es falso y, si bien es cierto que esta tecnología podría ser utilizada para reconstruir hechos noticiables⁴¹, la mayoría de las ocasiones se usa para la desinformación y, por ende, pierde uno de los requisitos de ponderación: la veracidad⁴². Por lo que se refiere a la libertad de expresión, dependerá de la relevancia pública de la opinión, expresión, juicio de valor, etc., siempre que no contengan expresiones difamatorias o injuriosas. En tal caso, deberá analizarse en qué situaciones deberá prevalecer el derecho a la libre expresión frente al derecho al honor como, por ejemplo, así sucede en las sátiras o caricaturas, al igual que sucede en el derecho a la imagen y voz de la persona⁴³.

3.1.3. Exclusión de la ilegitimidad de la injerencia de estos derechos

A) *El consentimiento del uso del deepfake*

El primer presupuesto legitimador que establece el artículo 2.2 de la LO 1/1982 es el consentimiento del titular de los derechos afectados: «No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso [...]». Ahora bien, por consentimiento expreso no debe entenderse que ha de prestar el consentimiento formalmente, sino que este sea inequívoco mediante actos concluyentes que expresan tal voluntad⁴⁴. Tomando en consideración el contexto de la sociedad digital en la que vivimos, podemos ver que el citado consentimiento

³⁹ Moliner Navarro, 2007: 29-37; Ysás Solanes, 2013: 839.

⁴⁰ Gutiérrez García, 2024: 166.

⁴¹ Gutiérrez García, 2024: 167.

⁴² Por información veraz, debe entenderse proporcionar información sobre unos hechos que pretenden ser ciertos (Moliner Navarro, 2007: 51).

⁴³ Gutiérrez García, 2024: 167.

⁴⁴ STS núm. 1116/2002, de 25 noviembre 2002, FJ 1 [RJ 2002\10274].

expreso también puede darse a través de unos nuevos «usos sociales» generados en las redes sociales. En efecto, la STS 907/2024, de 24 de junio⁴⁵ consideró que existía consentimiento para la publicación de unas fotografías en la red social de Facebook, dado que la demandante había interactuado con el contenido de dicha publicación pulsando “Me gusta”, demostrando así que estaba conforme con dicho contenido y sin que sea necesario que acepte la publicación de cada imagen por separado, dado que todos ellos eran de índole similar.

El consentimiento ha de prestarse para cada acto concreto, esto es, el hecho de consentir la captación de la imagen no viene a significar la publicación de la misma. Además, el consentimiento dado para un uso o finalidad determinada no cabe hacerlo extensible a otros fines o usos no autorizados⁴⁶, tal y como se advirtió en la STS 27/2020, de 24 de febrero⁴⁷: «El consentimiento solo ampara aquello que constituye el objeto de la declaración de voluntad. El titular del derecho fundamental debe autorizar el concreto acto de utilización de su imagen y los fines para los que la otorga. El consentimiento prestado, por ejemplo, para la captación de la imagen no se extiende a otros actos posteriores, como por ejemplo su publicación o difusión. De la misma manera debe entenderse que la autorización de una concreta publicación no se extiende a otras, ya tengan la misma o diversa finalidad que la primigenia. Tampoco el permiso de uso otorgado a una persona determinada se extiende a otros posibles destinatarios. En definitiva, hay que entender que no puede reputarse como consentimiento indefinido y vinculante aquel que se prestó inicialmente para una ocasión o con una finalidad determinada». Así las cosas, el hecho de que una persona suba una imagen a una red social no significa que se haya prestado el consentimiento para hacer uso de esa imagen a partir de la cual generar otra nueva imagen ficticia⁴⁸.

Por tanto, si la persona titular de los derechos al honor, de la imagen o de la voz presta el consentimiento para la creación o publicación de *deepfakes*, ello

⁴⁵ STS núm. 907/2024, de 24 de junio, FJ 2 [JUR 2024\190594]: «Dados los usos sociales generados por las redes sociales, una actuación como la de la demandante, consintiendo en ser fotografiada por su marido cuando sabía que este era titular de una cuenta de Facebook, clicando “me gusta” o “¡adore” en varias de las fotografías colocadas en el muro de dicha cuenta de Facebook en las que aparecía la demandante (lo que además demuestra que accedía a dicha cuenta con regularidad), sin haber objetado en momento alguno a dicha conducta de su marido ni haberle solicitado que retirara las fotografías de su cuenta de Facebook, debe considerarse, apreciada en su conjunto, como una actuación concluyente demostrativa de consentimiento a que su imagen fuera no solo captada sino también publicada en la cuenta de Facebook por su marido».

⁴⁶ De Verda y Beamonte, 2017: 18-19.

⁴⁷ STC núm. 27/2020, de 24 de febrero, FJ 4 [RTC 2020\27].

⁴⁸ Presno Linera, M. A. (2022). *Derechos fundamentales e inteligencia artificial*. Marcial Pons. 44-45.

excluye la ilegitimidad de la intromisión. Ahora bien, debe tenerse en cuenta, tal y como se advirtió previamente, que la creación de las ultrasuplantaciones consta de dos momentos (el del entrenamiento de la red y el de la generación del contenido por esta) y que en ambos ha de constar el consentimiento.

Sin perjuicio de lo anteriormente expuesto, el consentimiento puede ser revocado y ello supondrá que desaparezca, en principio, la legitimación de la injerencia en estos derechos. A este respecto, De Verda y Beamonte considera que, si bien es cierto que los titulares de estos derechos pueden prestar su consentimiento a cambio de un precio, ello no significa que estos derechos sean derechos patrimoniales, por el contrario, se trata de derechos indisponibles⁴⁹. Así las cosas, el titular de los derechos puede revocar su consentimiento y, además, esta revocación se extenderá a otros terceros posibles cesionarios⁵⁰. Ahora bien, como dispone el artículo 2.3 del mismo texto normativo, el consentimiento es revocable en cualquier momento, sin perjuicio de los posibles daños y perjuicios ocasionados, incluyendo las «expectativas justificadas».

Por lo que a los menores de edad se refiere, debe tomarse en consideración su situación particular. Así, el artículo 3 de la LO 1/1982 distingue a los menores de edad⁵¹ dependiendo de sus condiciones de madurez: por un lado, si el menor tiene madurez suficiente podrá autorizar por sí mismo la intromisión a su derecho al honor, a la imagen y a la voz; por el contrario, si el menor no tiene las condiciones de madurez suficiente, será su representante legal el que debe otorgar el consentimiento por escrito, previa puesta en conocimiento al Ministerio Fiscal, que puede oponerse en el plazo de 8 días, en cuyo caso resolverá el Juez⁵². No obstante, tal y como destaca la Instrucción de la Fiscalía General del Estado 2/2006, de 15 de marzo, sobre el Fiscal y la protección del derecho al honor, intimidad y propia imagen de los menores, las ocasiones en las que los representantes legales de los menores de edad

⁴⁹ De Verda y Beamonte, 2017: 17-18.

⁵⁰ De Verda y Beamonte, J. R. (2007b). El consentimiento como causa de exclusión de la ilegitimidad de la intromisión. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 239-253). Aranzadi. 252-253; De Verda y Beamonte, 2017: 18-19.

⁵¹ Este precepto también se refiere a los «incapaces», sin embargo, esta norma debe interpretarse conforme a los principios incorporados por la Convención sobre los derechos de las personas con discapacidad, ratificado en Nueva York el 13 de diciembre de 2006, así como a la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica.

⁵² Esta excepción a la representación de quien ejerce la patria potestad se encuentra en sintonía con la que se encuentra en el artículo 162.1º del Código Civil: «Los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. Se exceptúan: 1º Los actos relativos a los derechos de la personalidad que el hijo, de acuerdo con su madurez, pueda ejercitar por sí mismo. No obstante, los responsables parentales intervendrán en estos casos en virtud de sus deberes de cuidado y asistencia».

prestan tal consentimiento por escrito y ponen en conocimiento al Ministerio Fiscal son muy escasas, pero que ello no debe suponer la impugnación de negocios o actos cuando estos sean respetuosos con los menores, aunque se hayan incumplido los citados requisitos formales.

Ahora bien, como bien advierte De Verda y Beamonte, en los casos de los menores de edad la prestación del consentimiento, ya sea del propio menor o de sus representantes legales, no es el único requisito que debe cumplirse para la exclusión de la ilegítima intromisión a los derechos objeto de estudio, sino que, además, deben cumplir el presupuesto adicional establecido en el artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil: que no menoscabe la honra o reputación del menor o que sea contrario a sus intereses⁵³. A modo de ejemplo, a pesar de que el menor (maduro) o sus representantes legales accedan a la creación de *deepfakes* pornográficos, esta intromisión será considerada ilegítima en tanto que atentan contra su honra o reputación.

B) Las intromisiones autorizadas por Ley

Tras el análisis del consentimiento del afectado, resulta conveniente el estudio de otras causas de legitimidad que autorizan la intromisión en los derechos objeto de análisis. Estas se encuentran en el artículo 8 de la LO 1/1982 y, a continuación, se abordará cada apartado de este precepto, así como su aplicación en las ultrasplantaciones.

En primer lugar, el artículo 8.1 de la LO 1/1982 menciona ciertas intromisiones que son consideradas legítimas de los derechos que aborda el texto normativo: «1. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante». A este respecto, debe advertirse que no será suficiente con la prevalencia del interés histórico, científico o cultural, sino que, además, esta intromisión deberá ser necesaria para poder alcanzar tales intereses⁵⁴.

Por su parte, el apartado segundo del mismo precepto menciona unos supuestos específicos que se aplican únicamente en el derecho a la propia imagen. Estos límites se justifican en la necesidad de ponderar este derecho

⁵³ De Verda y Beamonte, J. R. (2009). Resarcimiento del daño moral por intromisiones consentidas en el derecho a la propia imagen de menores (en relación al caso Marta del Castillo), *Diario La Ley* (7171), 4-5.

⁵⁴ De Verda y Beamonte, 2007c: 257.

con la libertad de expresión e información, con el fin de que la sociedad democrática pueda formarse una opinión a través de una información veraz y el contraste de opiniones⁵⁵: «2. En particular, el derecho a la propia imagen no impedirá:

- a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público.
- b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.
- c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoría.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza».

Para el correcto estudio, conviene el análisis pormenorizado de cada uno de ellos a los efectos de poder, posteriormente, extraer conclusiones acerca del uso de la tecnología *deepfake*.

La primera intromisión legítima al derecho a la imagen es la «captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público». A este respecto, destacan dos requisitos: por un lado, que la persona captada tenga carácter público y, por el otro, que la imagen se capte en un acto público. Sin embargo, como se ha advertido previamente, el objeto de la legitimación de esta intromisión al derecho a la propia imagen es la libertad de información. De este modo, si la imagen no tiene un interés informativo (por ejemplo, porque se utiliza con fines publicitarios o crematísticos) o este no tiene interés general, la intromisión será ilegítima⁵⁶. En relación de esta causa de legitimidad con el uso de las ultrasuplantaciones, se ha considerado que no es posible que sean legítimas porque se trata de imágenes falsas⁵⁷ y, si bien es cierto que la veracidad no juega un papel fundamental como sucede con el derecho al honor y a la intimi-

⁵⁵ De Verda y Beamonte, 2007c: 258-259.

⁵⁶ De Verda y Beamonte, 2007c: 263-264; De Verda y Beamonte, 2017: 22-23. Castilla Barea, M. (2011). *Las intromisiones legítimas en el derecho a la propia imagen: estudio de las circunstancias que legitiman la intromisión en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, Thomson Reuters Aranzadi, 328-337.

⁵⁷ Gutiérrez García, 2024: 162 y Trujillo Cabrera, 2024: 96.

dad personal, debe tomarse en consideración que el fundamento de la consideración de legítima esta intromisión es la formación de una opinión pública a partir de una información veraz⁵⁸, presupuesto del que carecen los *deepfakes*.

La segunda causa de legitimación de la intromisión al derecho a la propia imagen es la «utilización de la caricaturade dichas personas [las que ejerzan un cargo público o una profesión de notoriedad], de acuerdo con el uso social». Por caricatura ha de entenderse la representación gráfica en la que se deforma la imagen de una persona en clave humorística y con carácter crítico o satírico en el ejercicio de la libertad de expresión⁵⁹. Al hilo de las caricaturas, conviene analizar, asimismo, que es lícito el uso de las imitaciones o de los dobles (tanto de la imagen, como de la voz) de personajes públicos cuando estos no induzcan a confusión, con fines humorísticos, pero nunca comerciales o crematísticos⁶⁰. De Verda y Beamonte ha considerado que no existirá confusión cuando exista una advertencia de que no se trata de la persona pública a la que es similar. Sin embargo, sí será ilegítima, a pesar de que exista tal advertencia cuando se asocia el producto al personaje famoso al que el doble se asemeja⁶¹. Por lo que al estudio de las ultrafalsificaciones se refiere, particularmente interesante resulta la STS 185/2006, de 7 de marzo de 2006⁶² en la que se abordó un fotomontaje en el que se había puesto la cara de una mujer famosa en un cuerpo semidesnudo de otra mujer. En tal caso, el Tribunal consideró que no nos encontrábamos ante una caricatura en tanto que no se mostraba una deformación de la cara ni del cuerpo, y porque la composición parecía ser de la misma persona. En definitiva, cabe concluir que no se considerará caricatura cuando se trata de una reproducción gráfica de una persona en la que esta no aparezca deformada o la deformación no sea fácilmente apreciable⁶³. Así las cosas, tomando en consideración que las ultrafalsificaciones pretenden crear

⁵⁸ Castilla Barea, 2011: 338.

⁵⁹ De Verda y Beamonte, 2007c: 266; De Verda y Beamonte, 2017: 26.

⁶⁰ En cuanto a la imagen: De Verda y Beamonte, 2007c: 270-272; De Verda y Beamonte, 2007d: 639; De Verda y Beamonte, 2017: 29. Por lo que se refiere a las imitaciones de voz: De Verda y Beamonte, 2007a: 165-167; De Verda y Beamonte, 2007d: 639-640; Ammerman Yebra, 2021: 237-238; Trujillo Cabrera, 2024: 98-99.

⁶¹ De Verda y Beamonte, 2017: 20.

⁶² STS núm. 185/2006, de 7 de marzo de 2006, FJ 4 [RJ 2006\1579]: «en el fotomontaje publicado el rostro era el de la demandante sin deformación alguna, es decir, sus facciones, el elemento por el que más identificable es una persona, y el cuerpo semidesnudo era el de otra mujer, por ende tampoco deformado ni ridiculizado sino, lejos de ello, conjuntado con el rostro de la demandante de un modo tan perfecto que los dos elementos de la composición parecían pertenecer a una misma persona».

⁶³ De Verda y Beamonte, 2007c: 263-264.

De Verda y Beamonte, J. R. (2007d). 1971 Sentencia de 7 de marzo de 2006: Objeto: Intromisión ilegítima en el derecho a la propia imagen, originada por la publicación de un fotomontaje. Concepto de caricatura y límites de la autorización legal, *Cuadernos Civitas de jurisprudencia civil* (74), 635.

un contenido casi idéntico al de la persona real, podemos concluir que tampoco encajarían en el concepto de caricatura, dado que no nos encontramos ante ninguna deformación fácilmente apreciable⁶⁴. Sin embargo, Gutiérrez García considera que los *deepfakes* sí que podrían considerarse intromisiones legítimas en virtud de las caricaturas siempre y cuando la finalidad sea satírica o humorística y el contenido falso sea fácilmente identificable, a pesar de que no exista una deformación de la imagen o de la voz de la persona, en cuyo caso, jugaría un papel importante la advertencia o identificación de este como un contenido falso⁶⁵.

La tercera causa de legitimación de la intromisión al derecho a la imagen es que «la información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesorio». Sin embargo, se ha cuestionado que los *deepfakes* puedan ampararse a este respecto, en tanto que, como ya se ha advertido previamente, aunque podría considerarse interesante la recreación de un suceso, sería dudosa la utilización de la imagen de las personas para este fin (tanto de los personajes públicos o con cargos de notoriedad, como de los que no lo tengan), dado que lo relevante no es la imagen, sino el suceso o el acaecimiento público⁶⁶.

3.1.4. La utilización del *deepfake post mortem*

Si bien es cierto que los derechos de la personalidad se extinguen con la muerte de su titular (art. 32 CC), el Preámbulo de la LO 1/1982 reconoce una protección de la memoria de la persona fallecida: «Aunque la muerte del sujeto de derecho extingue los derechos de la personalidad la memoria de aquél constituye una prolongación de esta última que debe también ser tutelada por el Derecho». Así pues, la Exposición de Motivos de esta norma equipara memoria a la prolongación de la personalidad del difunto⁶⁷. Sin embargo, se ha considerado que el hecho de que la legitimación activa e indemnización la tengan los familiares y no los herederos del difunto, demuestra que el daño reparado no es la tutela de los derechos de la personalidad del fallecido, sino el daño moral de los familiares⁶⁸.

⁶⁴ En este sentido, Trujillo Cabrera, 2024: 97-98.

⁶⁵ Gutiérrez García, 2024: 163-165.

⁶⁶ Gutiérrez García, 2024: 165.

⁶⁷ Ysás Solanes, 2013: 869.

⁶⁸ De Verda y Beamonte, 2007a: 177-178; Cobas Cobiella, M. E. (2011). Protección «post mortem» de los derechos de la personalidad. Algunas notas sobre el tema. En J. R. de Verda y Beamonte (Coord.), *El Derecho a la Imagen desde todos los Puntos de vista* (pp. 199-216). Aranzadi. Revista Aranzadi de Derecho y Nuevas Tecnologías, Monografía. 206-207.

En cuanto al *deepfake* se refiere, como se ha advertido previamente, se ha visto como algunos personajes famosos han «cobrado vida» para promocionar cervezas, competiciones deportivas o para finalizar películas inacabadas, por ello, no debe desconocerse que ante estas situaciones también se pueden emplear medidas de protección. A este respecto, dependerá del momento de la lesión, si el *deepfake* es creado tras el fallecimiento, en tal caso las personas mencionadas en el artículo 4 del citado texto normativo (el designado en testamento, cónyuge, descendientes, ascendientes y hermanos o el Ministerio Fiscal) podrán ejercitar la acción y el plazo de caducidad será de 4 años. En estos casos, la indemnización corresponderá al cónyuge, descendientes, ascendientes o hermanos y, en defecto de ellos, a sus causahabientes, en proporción a lo que la sentencia estime que han sido afectados. Así las cosas, pueden ser indemnizadas las personas mencionadas a pesar de que no hayan ejercitado la acción.

La otra situación que puede ocurrir es que la ultrasuplantación sea creada antes del fallecimiento del afectado y las acciones fueron iniciadas por el ofendido, estas pueden ser continuadas por las personas designadas por el fallecido, cónyuge, descendientes, ascendientes y hermanos que vivan al tiempo del fallecimiento, así como al Ministerio Fiscal ante la falta de todos los anteriores (art. 6.2 LO 1/1982, en relación con el artículo 4 de la misma norma). Si, por el contrario, la ofensa se dio durante la vida del titular del derecho, pero no pudo ejercitar sus acciones, estas podrán ejercitarse por las mismas personas mencionadas anteriormente, pero en cuyo caso será necesario que demuestren que el perjudicado desconocía la lesión⁶⁹.

Sin perjuicio de lo anteriormente expuesto, si bien es cierto que la LO 1/1982 protege la memoria de las personas tras su fallecimiento, nada se dice al respecto de la transmisibilidad de los componentes patrimoniales de los derechos de la personalidad. Sin embargo, sería posible que el testador designara a los beneficiarios de la explotación económica de sus derechos de la personalidad tras su muerte⁷⁰.

3.2. LA IMAGEN Y VOZ COMO DATOS DE CARÁCTER PERSONAL EN EL USO DEL DEEPFAKE

Otra problemática jurídica que implica el uso de la tecnología *deepfake* es la referido a los datos de carácter personal. Y es que la imagen (y conforme se ha defendido anteriormente, también la voz), además de ser derechos de la personalidad por sí mismos, encajan en la definición que da el artículo 4.1) del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27

⁶⁹ Ysás Solanes, 2013: 869.

⁷⁰ Ammerman Yebra, 2021: 175-178.

de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos, en adelante, RGPD): «toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». Asimismo, la protección de datos está tutelada como derecho fundamental en España en virtud del artículo 18.4 de la Constitución Española: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

En cuanto a las bases de legitimación del tratamiento de los datos personales en los supuestos de *deepfake* que contempla el artículo 6.1 del RGPD únicamente parece encajar el uso de esta tecnología en la prestación del consentimiento por parte del interesado del primer inciso del citado precepto legal⁷¹. En este caso, por consentimiento del interesado ha de entenderse «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara afirmativa, el tratamiento de datos personales que le conciernen» (art. 4.11 del RGPD). Aunque este precepto no lo menciona expresamente, parece interpretarse que el consentimiento ha de ser expreso como parece desprenderse de los considerandos 32⁷² y 42⁷³ del RGPD⁷⁴.

⁷¹ Trujillo Cabrera, 2024: 101.

⁷² «El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta».

⁷³ «Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo (1), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del

Sin embargo, debe reconocerse que es en escasas ocasiones cuando el consentimiento a la cesión de datos se da tras una lectura detenida de las condiciones de privacidad, en tanto que muchas veces la prestación de este consentimiento viene condicionada con la utilización de un servicio o porque la petición es urgente o engañosa o, incluso, porque es más fácil consentir que el procedimiento que debe realizarse para rechazar dicha cesión de datos⁷⁵.

Respecto a los menores de edad, cabe destacar que el RGPD considera que será lícito el tratamiento de los datos personales por medio del consentimiento si este tiene al menos 16 años, en caso contrario, deberá ser autorizado por el titular de la patria potestad o tutela del menor (artículo 8.1 del RGPD). Ahora bien, este mismo precepto permite a los Estados Miembros rebajar este límite de edad hasta un máximo de 13 años. En el supuesto de España, la LOPD permite que los menores puedan prestar consentimiento para el tratamiento de los datos personales a partir de los 14 años (artículo 7⁷⁶). Además, esta información y comunicación ha de proporcionarse en un lenguaje claro y sencillo y de fácil comprensión (considerando 58). Sin perjuicio de lo anteriormente expuesto, se ha criticado el hecho de que, a pesar de la existencia de tal obligación, no se imponga la verificación de la edad de las personas en redes sociales, ni tampoco la participación efectiva de quien ejerce la patria potestad⁷⁷.

En cuanto a la revocación del consentimiento, debe tomarse en consideración el artículo 7.3 del RGPD que señala: «El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consenti-

tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. [...]».

⁷⁴ En este sentido, Arnau Moya, F. (2019). La jurisprudencia del Tribunal Europeo de Derechos Humanos en materia de derechos de la personalidad e internet. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 11-47). Tirant lo Blanch; Trujillo Cabrera, 2024: 102.

⁷⁵ Mattace, G. (2024). La protección de los datos personales de los niños en el espacio digital, *Actualidad Jurídica Iberoamericana* (20), 1428-1429; De Barrón Arniches, P. (2024). Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela. *Revista de Derecho civil* (XI, núm. 1). 170-178.

⁷⁶ «1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela».

⁷⁷ Matacce, 2024: 1428.

miento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo». Asimismo, habrá que ser completado con el considerando 42: «[...]El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno». Aunque esto puede resultar contradictorio con el artículo 2.3 de la LO 1/1982, analizado previamente, como bien advierte Trujillo Cabrera, es perfectamente compatible, en tanto que el agravio se refiere a la retirada del consentimiento, sin perjuicio de que sí que se puedan indemnizar otros perjuicios que se hubieran podido causar, tal y como reconoce el artículo 2.3 de la LO 1/1982⁷⁸.

4. EL PAPEL DE LA ADVERTENCIA EN EL USO DEL *DEEPPFAKE*

Tal y como se ha defendido, el uso del *deepfake* afecta a los derechos de la personalidad anteriormente mencionados. Sin embargo, el tratamiento que ha dado el Reglamento de Inteligencia Artificial y el Reglamento de Servicios Digitales a esta tecnología es, sencillamente, como un sistema sometido a obligaciones de transparencia, esto viene a significar que resulta preceptiva la mención de que se trata de un contenido generado por Inteligencia Artificial. A partir de tales premisas, cabe cuestionarse si esta advertencia supone un nuevo presupuesto legitimador que permitiría el uso de esta tecnología con la simple advertencia de que se trata de un contenido generado mediante Inteligencia Artificial o si, por el contrario, requiere de otros presupuestos legitimadores.

A nuestro modo de ver, el Reglamento de Inteligencia Artificial junto con el Reglamento de Servicios Digitales han clasificado el riesgo del *deepfake* desde la perspectiva de la desinformación y las noticias falsas que pueden generar, pero no se ha planteado desde el punto de vista de la vulneración a otros derechos fundamentales. No obstante, como se ha advertido previamente, el riesgo de las ultrafalsificaciones va más allá de la desinformación y, por ello, incluso algún autor reconoce la posibilidad de haber sido clasificado como un sistema de inteligencia artificial de mayor riesgo por cuanto que afectan a los derechos fundamentales⁷⁹.

⁷⁸ Trujillo Cabrera, 2024: 103.

⁷⁹ Gutiérrez García, 2024: 180-181.

Ahora bien, el Reglamento de Inteligencia Artificial, en su Considerando 134, toma en cuenta que la advertencia debe conjugarse con las garantías adecuadas para los derechos y libertades de terceros⁸⁰. Así las cosas, consideramos que la advertencia no puede suponer un presupuesto legitimador por sí mismo, por cuanto que esto dejaría desprotegidos los derechos fundamentales anteriormente analizados. Por ello, cabe cuestionarse entonces, cuál es el papel que juega la advertencia en el uso de las ultrasuplantaciones.

A este respecto, la advertencia puede jugar un papel fundamental cuando las creaciones de *deepfake* supongan un riesgo de confusión a los receptores, así como para la desinformación⁸¹. De este modo, la advertencia será crucial para que un contenido pueda ser considerado como caricatura, por ejemplo, cuando, mediante el uso de la tecnología *deepfake*, este no sea fácilmente identificable como falso. Sin embargo, debe tomarse en consideración que, además de la advertencia, debe existir otro presupuesto legitimador de la injerencia del derecho de la personalidad de los previstos legalmente.

Sin perjuicio de lo anteriormente expuesto, la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de inteligencia artificial, tal y como se advirtió previamente, pretende modificar, entre otras leyes, la LO 1/1982 al incorporar un apartado 9º al artículo 7. Este considera ilegítima la difusión y utilización de la imagen o de los audios de voz de una persona cuando no exista consentimiento de esta. Hasta el momento, estamos de acuerdo, sin embargo, el precepto

⁸⁰ «Además de las soluciones técnicas utilizadas por los proveedores del sistema de IA, los responsables del despliegue que utilicen un sistema de IA para generar o manipular un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeje notablemente a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos (ultrasuplantaciones) deben también hacer público, de manera clara y distinguible, que este contenido ha sido creado o manipulado de manera artificial etiquetando los resultados de salida generados por la IA en consecuencia e indicando su origen artificial. El cumplimiento de esta obligación de transparencia no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida obstaculiza el derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, *con sujeción a unas garantías adecuadas para los derechos y libertades de terceros*. En tales casos, la obligación de transparencia en relación con las ultrasuplantaciones establecida en el presente Reglamento se limita a revelar la existencia de tales contenidos generados o manipulados de una manera adecuada que no obstaculice la presentación y el disfrute de la obra, también su explotación y uso normales, al tiempo que se conservan la utilidad y la calidad de la obra. Además, también conviene prever una obligación de divulgación similar en relación con el texto generado o manipulado por una IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por la IA haya sido sometido a un proceso de revisión humana o de control editorial y que una persona física o jurídica ejerza la responsabilidad editorial de la publicación del contenido». La cursiva es nuestra.

⁸¹ Gutiérrez García (2024): 164-165.

añade que la advertencia de que dicho contenido se ha generado mediante Inteligencia Artificial excluye la ilegitimidad de la intromisión. Ello, a nuestro entender, no debería ser suficiente, sino que deberían existir otras causas de legitimidad por las que ceden los derechos anteriormente mencionados, como que exista otro derecho fundamental en conflicto. De este modo, los derechos a la propia imagen, a la voz y al honor deberían ser ponderados (e incluso ceder), por ejemplo, con la libertad de expresión, pero no bajo cualquier circunstancia, sino cuando tienen una relevancia pública y no contenga expresiones difamatorias o injuriosas.

En definitiva, consideramos que la advertencia es un requisito para el uso del *deepfake* que, además, debe conjugarse con la tutela de los derechos de la personalidad que hemos abordado con carácter previo. De este modo, la mera presencia de una advertencia no supondría un presupuesto legitimador de las inferencias de los derechos fundamentales por sí mismo.

5. MECANISMOS DE PROTECCIÓN

Tal y como se ha analizado, el uso del *deepfake* puede generar una infracción tanto en los derechos de la personalidad como el honor, la imagen o la voz, a la vez que puede infringir la protección de datos personales de una persona en tanto que la imagen y la voz se consideran datos personales. De este modo, la persona afectada en sus derechos puede optar por la tutela de estos por cualquiera de las vías que existen de protección, e incluso, en algunos casos, de manera cumulativa o alternativa⁸². En lo que a este estudio se refiere, nos centraremos en las acciones de responsabilidad civil.

⁸² SAN, sala de lo contencioso-administrativo, de 2 de enero de 2013, FJ 4 [RJCA 2013\100]: «Habiendo también reiterado la Sala [...] la compatibilidad del procedimiento sancionador o de tutela seguidos ante la AEPD con los procesos civiles promovidos al amparo de la Ley Orgánica 1/1982». En este mismo sentido, Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución* (34), 223-225; Castilla Barea, M. (2019). Algunos casos de vulneración del derecho a la protección de datos personales en el entorno de las redes sociales y de las aplicaciones de mensajería instantánea. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 49-82). Tirant lo Blanch: «Pues bien, en estos casos en los que una misma conducta o supuesto de hecho constituya una vulneración simultánea del derecho a la protección de datos personales y de uno de esos otros derechos mencionados, será decisión libre del titular de los derechos afectados instar la aplicación exclusiva de solo una de las leyes aplicables -LOPD o LODH- o acumular pretensiones diversas de protección de sus derechos, debiendo en este último caso -eso sí-, articular cada una de ellas por la vía procedente».

5.1. TUTELA DE LOS DERECHOS DE LA PERSONALIDAD PROTEGIDOS EN LA LO 1/1982

Por lo que se refiere a los mecanismos de protección de los derechos protegidos por la LO 1/1982, a nuestro interés, el derecho al honor y a la propia imagen (y a la voz), cabe destacar que el artículo 9 de dicha norma prevé una protección preventiva del daño, así como mecanismos de resarcimiento y de cesación tras la causación de la intromisión. Así, los objetivos de dicho precepto son el restablecimiento del perjudicado en el pleno disfrute de sus derechos, la prevención de intromisiones inminentes o posteriores, el resarcimiento de los daños y perjuicios de las intromisiones ya causadas y, por último, el restablecimiento del lucro obtenido por la intromisión ilegítima (artículo 9.2 LO 1/1982).

Por lo que se refiere a la responsabilidad civil, es importante destacar que el apartado tercero de dicho precepto⁸³ presume el perjuicio ocasionado tras la intromisión⁸⁴. Ahora bien, ello no exime de demostrar otros extremos de la responsabilidad civil, como la cuantificación del daño⁸⁵. Sin embargo, no realiza dicho precepto mención alguna en relación con el criterio de atribución de responsabilidad, esto es, si nos encontramos ante una responsabilidad por culpa o por riesgo. Ante esta disyuntiva, Atienza Navarro considera que en tal caso deberá atenderse a criterios diversos en atención a si las actividades realizadas implican un riesgo por sí mismas o no lo implican⁸⁶.

⁸³ «La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido».

⁸⁴ En cuanto al alcance de dicha presunción, se considera que esta únicamente alcanza a los daños morales, pero no a los patrimoniales. En este sentido, Atienza Navarro, M. L. (2011). Algunas cuestiones acerca de la responsabilidad civil por intromisiones ilegítimas en el Derecho a la propia imagen. En J. R. de Verda y Beamonte (Coord.), *El Derecho a la Imagen desde todos los Puntos de vista* (pp. 141-165). Aranzadi. Revista Aranzadi de Derecho y Nuevas Tecnologías, Monografía. 144-145 y Ysás Solanes, 2013: 875.

En cuanto al carácter de dicha presunción, esto es, *iuris tantum* o *iuris et de iure*, la doctrina se encuentra dividida entre los que optan por la primera opción, tales como: Atienza Navarro, 2011: 146-156; y los que entienden que nos encontramos ante una presunción *iuris et de iure*, a modo de ejemplo, Rubí Puig, 2019: 223.

⁸⁵ Jerez Delgado, C. (2019). El daño moral en internet: en particular, la responsabilidad civil por la lesión de los derechos al honor, intimidad y propia imagen. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 309-346). Tirant lo Blanch.

⁸⁶ Atienza Navarro, 2011: 157-159.

Finalmente, cabe recordar que también puede resarcirse por una intromisión posterior a la muerte, en tales supuestos, el artículo 9.4⁸⁷ de dicho texto legal determina quiénes serán los acreedores de la indemnización. Así, si la intromisión se realiza tras la muerte del ofendido, el importe de la indemnización por el daño moral corresponderá al cónyuge, descendientes, ascendientes y hermanos que viviesen al tiempo del fallecimiento y, en defecto de todos ellos, a sus causahabientes en la proporción en que la sentencia determine que han sido afectados. Si, por el contrario, la ofensa se hizo en vida del ofendido, pero este no pudo ejercitar tales acciones, la indemnización se entenderá comprendida en la herencia del perjudicado.

5.2. TUTELA DE LOS DATOS DE CARÁCTER PERSONAL

En cuanto se refiere a la protección de los datos personales, el titular del derecho puede optar por dos vías específicas de conformidad con el RGPD: la primera de ellas es la tutela administrativa ante la Agencia Española de Protección de Datos (en adelante, AEPD) o ante los tribunales contenciosos-administrativos, que perseguirán la sanción del infractor (arts. 77-79 RGPD); la segunda de las vías ofrecidas es la acción de representación para la defensa de los intereses colectivos relacionados con la privacidad de las persona (art. 80 RGPD). Además de las anteriormente mencionadas, existe una tercera vía de tutela contemplada en el artículo 82 RGPD, estas son, en efecto, las acciones civiles privadas, en concreto, las acciones de responsabilidad civil.

Por lo que se refiere a la vía administrativa, ya sea mediante una reclamación ante la AEPD o ante los órganos contenciosos administrativos, se pretende la imposición de una sanción al infractor. Ahora bien, este sistema se ha considerado insuficiente en tanto que no siempre se imponen sanciones y, en el caso de imponerse, estas no suponen unas cantidades que resulten gravosas para las grandes compañías tecnológicas, que consigan disuadir el incumplimiento de tales normas⁸⁸.

En cuanto a la segunda de las vías, esto es, el ejercicio de las acciones colectivas de protección señala el artículo 80 RGPD que «1. El interesado tendrá

⁸⁷ «El importe de la indemnización por el daño moral, en el caso de los tres primeros apartados del artículo cuarto, corresponderá a las personas a que se refiere su apartado dos y, en su defecto, a sus causahabientes, en la proporción en que la sentencia estime que han sido afectados. En los casos del artículo sexto, la indemnización se entenderá comprendida en la herencia del perjudicado.

En el caso del apartado cuatro del artículo cuarto, la indemnización corresponderá a los ofendidos o perjudicados por el delito que hayan ejercitado la acción. De haberse ejercitado por el Ministerio Fiscal, éste podrá solicitar la indemnización para todos los perjudicados que hayan resultado debidamente identificados y no hayan renunciado expresamente a ella».

⁸⁸ De Barrón Arniches, P. (2024). Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela. *Revista de Derecho civil* (XI, núm. 1). 180-181.

derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento».

De este modo, se ha contemplado esta vía como un mecanismo efectivo para garantizar los derechos protegidos frente a las grandes empresas tecnológicas por los mecanismos automatizados y las técnicas de recopilación de datos⁸⁹.

Finalmente, la última de las vías de protección contemplada en el RGPD son las acciones de tutela civil, esto es, las de responsabilidad civil, en concreto, el artículo 82⁹⁰ del RGPD⁹¹.

⁸⁹ De Barrón Arniches, 2024: 190.

⁹⁰ «1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de res-

En relación con esta norma, cabe advertir que, pese a que la ley otorga legitimación activa a «toda persona», en realidad, ha de circunscribirse a la víctima o al perjudicado por el tratamiento de datos personales⁹². Por su parte, los sujetos a los que debe exigirse responsabilidad, conforme al precepto, serán el responsable y el encargado del tratamiento, pero, además de los mencionados, se puede exigir tal responsabilidad al subencargado del tratamiento de datos y al representante en la Unión Europea⁹³.

Asimismo, en relación con el daño, el Tribunal de Justicia de la Unión Europea ha tenido la oportunidad de pronunciarse en la reciente STJUE de 4 de mayo de 2023⁹⁴. En la citada sentencia, el Tribunal advierte que no solo basta con la infracción de la norma para solicitar una indemnización conforme al artículo 82 RGPD, sino que, además, deben concurrir otros dos requisitos de manera acumulativa⁹⁵: la existencia de un daño y la prueba de una relación de causalidad⁹⁶. Asimismo, cabe destacar, conforme la misma resolu-

ponsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2».

⁹¹ Por lo que se refiere a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, únicamente se refiere a esta vía de tutela en el artículo 30.2 («Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados») remitiéndose al precepto anteriormente mencionado.

⁹² Es por ello por lo que Moreno Martínez, J. A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. En J. Ataz López, J. A. Cobacho Gómez (Coords.), *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillaumon, Tomo III* (pp. 515-567). Thomson Reuters Aranzadi. 522-523, propone la expresión «interesado» o «persona interesada» que integran tanto al perjudicado directo, como a las víctimas indirectas por dicho tratamiento.

⁹³ Moreno Martínez, 2021: 525. Sin embargo, considera que no podrá exigirse responsabilidad alguna al Delegado de Protección de Datos, dada la función de dependencia, en tanto que su responsabilidad queda subsumida en la de los sujetos responsables. Moreno Martínez, 2021: 525-532.

⁹⁴ STJUE, Sala Tercera, de 4 de mayo de 2023, caso UI contra Österreichische Post AG (caso 300/21) [TJCE 2023\79].

⁹⁵ «(32) Por una parte, del tenor de esta disposición [el art. 82 RGPD] se desprende claramente que la existencia “daños y perjuicios” o de “daños y perjuicios” que se han “sufrido” constituye uno de los requisitos del derecho a indemnización previsto en dicha disposición, al igual que la existencia de una infracción del RGPD y de una relación de causalidad entre dichos daños y perjuicios y esa infracción, de modo que estos tres requisitos son acumulativos.

(33) Por lo tanto, no puede considerarse que toda “infracción” de las disposiciones del RGPD dé lugar, por sí sola, al referido derecho a una indemnización a favor del interesado, tal como se define en el artículo 4, punto 1 de dicho Reglamento. Tal interpretación sería contraria al tenor del artículo 82, apartado 1, del citado Reglamento».

A estos requisitos, además, Rubí Puig, 2019: 201-202 añade la condición de responsable o encargado del tratamiento del reclamado.

⁹⁶ Al respecto del último requisito, De Barrón Arniches (2024: 183) destaca la contradicción de dicho pronunciamiento y el tenor literal del artículo 82.3 RGPD, que traslada la carga de la prueba al responsable o encargado del tratamiento. Por el contrario, Moreno Martínez (2021: 538-539),

ción, que la cuantificación del daño será calculada atendiendo a la normativa nacional de cada Estado Miembro.

No podemos finalizar este apartado sin hacer referencia a la compatibilidad de las acciones estudiadas: la de los derechos al honor, intimidad e imagen de la LO 1/1982 y la tutela prevista para la protección de datos personales⁹⁷. A este respecto, se ha considerado que resultaría más ventajoso acudir a los mecanismos previstos en el artículo 9 de la LO 1/1982, por cuanto que existe una presunción de la causación del daño moral que no existe en la normativa de protección de datos⁹⁸. De hecho, Rubí Puig destaca que, en el caso de plantearse una cuestión prejudicial ante el TJUE, posiblemente se considerara el uso de dicha presunción contraria al RGPD⁹⁹.

5.3. LA RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DIGITAL

Finalmente, cabe hacer mención a que, en muchas ocasiones, la creación de las ultrasuplantaciones que afectan a los derechos analizados anteriormente son publicados en foros de internet o en redes sociales incrementando así la difusión de este contenido. Es por ello por lo que resulta conveniente el análisis sucinto de la responsabilidad civil de los prestadores de servicios de la sociedad digital en estos supuestos, en concreto, de los prestadores de servicios de alojamiento o almacenamiento de datos y de las plataformas en línea. A este respecto, por servicio de alojamiento de datos debe entenderse el almacenamiento de «datos facilitados por el destinatario del servicio y a petición de este» (art. 3.g) iii del Reglamento de Servicios Digitales); mientras que por plataforma en línea ha de entenderse «un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que a esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento» (art. 3.i) del Reglamento de Servicios Digitales).

ya advertía con carácter previo al pronunciamiento del TJUE, que el daño debe probarse por el perjudicado, pero que, no obstante, es requerida la colaboración del responsable de los datos, en virtud del artículo 5.2 RGPD: «El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (“responsabilidad proactiva”)».

⁹⁷ Moreno Martínez, 2021: 555.

⁹⁸ Moreno Martínez, 2021: 556.

⁹⁹ Rubí Puig, 2019: 224.

En cuanto al sistema de responsabilidad de estas, debe mencionarse que el artículo 6 del Reglamento de Servicios Digitales¹⁰⁰ sobre la responsabilidad por el alojamiento de datos parte de la irresponsabilidad de los prestadores de servicios de intermediación, siempre que estos no tengan conocimiento efectivo de la actividad o información almacenada o que, si lo tiene, actúa con diligencia para retirar los datos o impedir el acceso a los mismos.

Por lo que se refiere a conocimiento efectivo, a diferencia de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), dicha exención de responsabilidad no se hace depender del papel pasivo del prestador de servicios intermediarios, sino que podrá beneficiarse de dicha exención siempre que esto no implique un conocimiento o un control del contenido ilícito¹⁰¹.

Asimismo, el artículo 7 del Reglamento de Servicios Digitales¹⁰², para evitar penalizar a aquellas plataformas que, de forma voluntaria, adopten me-

¹⁰⁰ «1. Cuando se preste un servicio de la sociedad de la información consistente en almacenar información facilitada por un destinatario del servicio, el prestador de servicios no podrá ser considerado responsable de la información almacenada a petición del destinatario, a condición de que el prestador de servicios:

a) no tenga conocimiento efectivo de una actividad ilícita o de un contenido ilícito y, en lo que se refiere a solicitudes de indemnización por daños y perjuicios, no sea consciente de hechos o circunstancias que pongan de manifiesto la actividad ilícita o el contenido ilícito, o

b) en cuanto tenga conocimiento o sea consciente de ello, el prestador de servicios actúe con prontitud para retirar el contenido ilícito o bloquear el acceso a este.

2. El apartado 1 no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o el control del prestador de servicios.

3. El apartado 1 no se aplicará con respecto a la responsabilidad, en virtud del Derecho en materia de protección de los consumidores, de las plataformas en línea que permitan que los consumidores celebren contratos a distancia con comerciantes, cuando dicha plataforma en línea presente el elemento de información concreto, o haga posible de otro modo la transacción concreta de que se trate, de manera que pueda inducir a un consumidor medio a creer que esa información, o el producto o servicio que sea el objeto de la transacción, se proporcione por la propia plataforma en línea o por un destinatario del servicio que actúe bajo su autoridad o control.

4. El presente artículo no afectará a la posibilidad de que una autoridad judicial o administrativa, de conformidad con el ordenamiento jurídico de un Estado miembro, exija al prestador de servicios que ponga fin a una infracción o que la impida».

¹⁰¹ López Richart, J. (2023). El Reglamento de Servicios Digitales: un nuevo marco de responsabilidad para los prestadores de servicios intermediarios en la Unión Europea. *Revista Aranzadi de Derecho y Nuevas Tecnologías* (62), 104.

¹⁰² «Investigaciones voluntarias por iniciativa propia y cumplimiento del Derecho.

No se considerará que los prestadores de servicios intermediarios no reúnen las condiciones para acogerse a las exenciones de responsabilidad a que se refieren los artículos 4, 5 y 6 por la única razón de que realicen, de buena fe y de modo diligente, investigaciones por iniciativa propia de forma voluntaria, o adopten medidas con el fin de detectar, identificar y retirar contenidos ilícitos, o bloquear el acceso a estos, o adoptar las medidas necesarias para cumplir los requisitos del Derecho

didadas voluntarias para detectar, identificar y retirar contenidos ilícitos o bloquear el acceso a los mismos, permite que puedan acogerse igualmente a la exención a la que se refiere el artículo 6 del mismo Reglamento.

Asimismo, el artículo 16 del Reglamento de Servicios Digitales ha introducido la obligación de establecer un sistema de notificación para los prestadores de servicios de alojamiento a los fines de facilitar que cualquier persona pueda notificar la presencia de contenidos ilícitos. Además, ello viene íntimamente relacionado con la exención de responsabilidad recogida en el artículo 6 de la citada norma, en tanto que esta comunicación permite considerar que la plataforma o el prestador de servicio de alojamiento ha tenido conocimiento efectivo del contenido ilícito¹⁰³.

Sin perjuicio de las modificaciones que se han introducido con ocasión de la entrada en vigor del Reglamento de Servicios Digitales, cabe destacar que la jurisprudencia española ya realizaba una interpretación amplia del concepto de «conocimiento efectivo» de la anterior Directiva sobre el comercio electrónico y su traslación al Derecho español a través de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Por este motivo, se llevó en ocasiones a responsabilizar, junto con los usuarios que realizaban actuaciones ilícitas en línea, a los prestadores de servicios de intermediación de alojamiento de datos en tanto que la denuncia podía ser considerada un conocimiento efectivo del ilícito¹⁰⁴.

6. CONCLUSIONES

Tras el análisis de las implicaciones de las ultrafalsificaciones en los derechos de la personalidad realizado en el presente trabajo, se pueden extraer las siguientes conclusiones:

1. Las ultrasuplantaciones, además de presentar grandes ventajas en la industria, también pueden suponer grandes riesgos, entre los que se encuen-

de la Unión y del Derecho nacional en cumplimiento del Derecho de la Unión, incluidos los requisitos establecidos en el presente Reglamento».

¹⁰³ López Richart, 2023: 106.

¹⁰⁴ Grimalt Servera, P. (2011). La responsabilidad civil de los prestadores de servicios de la sociedad de información. En J. R. de Verda y Beamonte (Coord.), *El Derecho a la Imagen desde todos los Puntos de vista* (pp. 167-197). Aranzadi. Revista Aranzadi de Derecho y Nuevas Tecnologías, Monografía. 187-196; Chaparro Matamoros, P. (2019). La responsabilidad de los prestadores de servicios de la información. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 99-142). Tirant lo Blanch.

tran la injerencia en los derechos de la personalidad a la propia imagen, la voz, el honor y a la protección de datos personales.

2. Para conocer si las intromisiones que se hacen en estos derechos son legítimas o ilegítimas, deberemos atender a las disposiciones clásicas de la legislación especial que tutelan dichos derechos, ahora bien, debemos interpretar dichas causas de legitimación y adaptarlas a la tecnología *deepfake*. Además, debe tenerse presente que las causas de legitimación deben encontrarse en todos los momentos de utilización de la tecnología, esto es, en el momento de entrenamiento de la red y en la generación y posterior publicación del contenido creado mediante Inteligencia Artificial.

3. Por lo que se refiere a la regulación específica en materia de ultrafalsificaciones, la legislación europea ha dado un tratamiento insuficiente a los riesgos que puede plantear esta tecnología en los derechos de la personalidad. Y ello por cuanto que, por un lado, considera la advertencia como un presupuesto legitimador de la injerencia de los derechos de la personalidad. Ello es conflictivo en tanto que, si bien es cierto que los efectos adversos del *deepfake* pueden ser mitigados mediante la advertencia de que nos encontramos ante un contenido manipulado o generado mediante Inteligencia Artificial, creemos que esto no reduce completamente las intromisiones ilegítimas en los derechos de la personalidad que pueden surgir del uso de la citada tecnología. En efecto, a nuestro entender, la advertencia, aunque puede tener un papel fundamental como requisito para la legitimación del uso del *deepfake* (por ejemplo, para las caricaturas), por sí misma no debería suponer una causa legitimadora, en tanto que ello supondría una injerencia desmedida en los derechos de la personalidad sin tener una justificación en la ponderación con otros derechos fundamentales, tal y como parece desprenderse del Considerando 134 del Reglamento de Inteligencia Artificial. Es por ello por lo que tampoco nos parece apropiado el tratamiento que hace de la cuestión la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de inteligencia artificial al otorgar a la advertencia el papel de causa legitimadora por sí misma. Así las cosas, a nuestro juicio, la advertencia debe considerarse un requisito de uso de las ultrasuplantaciones, pero deben concurrir, además, las causas legitimadoras previstas en la legislación especial a los efectos de que estas intromisiones puedan considerarse lícitas.

Por otro lado, el Reglamento de Servicios Digitales únicamente impone dicha advertencia a las plataformas en línea de muy gran tamaño, mientras que el Reglamento de Inteligencia Artificial lo impone al responsable del despliegue de los sistemas de Inteligencia Artificial, pero lo exime cuando el uso del *deepfake* no se enmarque en una actividad profesional. Esto, asimismo, lo

consideramos insuficiente en tanto que en muchas de las ocasiones en las que las ultrasuplantaciones han causado un perjuicio se han dado fuera del ámbito profesional (por ejemplo, las ultrafalsificaciones de menores o famosas desnudas). Por todo ello, entendemos que este deber de transparencia debería ser exigido a cualquier persona que genere un contenido falso mediante Inteligencia Artificial.

4. En cuanto a los mecanismos de reparación del daño, se advierte que, en ocasiones, una misma infracción puede ser abordada desde las acciones de la LO 1/1982 o desde la tutela que propone el RGPD. Ante este supuesto, se ha considerado más favorable las acciones de protección de la LO 1/1982 al existir una presunción del daño, que no se encuentra en el RGPD.

7. BIBLIOGRAFÍA.

- Ammerman Yebra, J. (2021). *El derecho a la propia voz como derecho de la personalidad*, Colex.
- Arnau Moya, F. (2019). La jurisprudencia del Tribunal Europeo de Derechos Humanos en materia de derechos de la personalidad e internet. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 11-47). Tirant lo Blanch.
- Atienza Navarro, M. L. (2011). Algunas cuestiones acerca de la responsabilidad civil por intromisiones ilegítimas en el Derecho a la propia imagen. En J. R. de Verda y Beamonte (Coord.), *El Derecho a la Imagen desde todos los Puntos de vista* (pp. 141-165). Aranzadi. Revista Aranzadi de Derecho y Nuevas Tecnologías, Monografía.
- Castilla Barea, M. (2011). *Las intromisiones legítimas en el derecho a la propia imagen: estudio de las circunstancias que legitiman la intromisión en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, Thomson Reuters Aranzadi.
- (2019). Algunos casos de vulneración del derecho a la protección de datos personales en el entorno de las redes sociales y de las aplicaciones de mensajería instantánea. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 49-82). Tirant lo Blanch.
- Chaparro Matamoros, P. (2019). La responsabilidad de los prestadores de servicios de la información. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 99-142). Tirant lo Blanch.
- Cobas Cobiella, M. E. (2011). Protección «post mortem» de los derechos de la personalidad. Algunas notas sobre el tema. En J. R. de Verda y Beamonte (Coord.), *El Derecho a la Imagen desde todos los Puntos de vista* (pp. 199-216). Aranzadi. Revista Aranzadi de Derecho y Nuevas Tecnologías, Monografía.

- De Barrón Arniches, P. (2024). Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela. *Revista de Derecho civil* (XI, núm. 1). 149-194.
- De Verda y Beamonte, J. R. (2007a). El derecho a la propia imagen. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 145-179). Aranzadi.
- (2007b). El consentimiento como causa de exclusión de la ilegitimidad de la intromisión. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 239-253). Aranzadi.
- (2007c). Las intromisiones en los derechos al honor, intimidad y propia imagen autorizadas por la Ley. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 255-277). Aranzadi.
- (2007d). 1971 Sentencia de 7 de marzo de 2006: Objeto: Intromisión ilegítima en el derecho a la propia imagen, originada por la publicación de un fotomontaje. Concepto de caricatura y límites de la autorización legal, *Cuadernos Civitas de jurisprudencia civil* (74), 629-642.
- (2009). Resarcimiento del daño moral por intromisiones consentidas en el derecho a la propia imagen de menores (en relación al caso Marta del Castillo), *Diario La Ley* (7171), 1-6.
- (2017). Los derechos fundamentales de la personalidad (al honor, a la intimidad y a la propia imagen) como categoría unitaria. *Revista Boliviana de Derecho* (23), 54-111.
- De Verda y Beamonte, J. R. y De las Heras Vives, L. (2019). Los derechos de la personalidad frente al sexting, streaming y otros fenómenos digitales: nuevos retos para su estudio, vigencia y protección en el siglo XXI. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 181-228). Tirant lo Blanch.
- García Rubio, M. P. (2013). Los derechos de la personalidad. En M. C. Gete-Alonso y Calera (Dir.) y J. Solé Resina (Coord.), *Tratado de derecho de la persona física. Tomo II* (pp. 597-631). Civitas-Aranzadi.
- García Ull, F. (2021). Deepfakes: el próximo reto en la detección de noticias falsas. *Anàlisi: Quaderns de Comunicació i Cultura* (64), 103-120.
- Gómez de Ágreda, Á., Feijóo, C., Salazar García, I. A. (2021). Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital. Deep fakes e inteligencia artificial. *Profesional de la información*, (30, 2). 1-24.
- Gutiérrez García, E. (2024). *Inteligencia Artificial y derechos fundamentales. Hacia una convivencia en la era digital*. Colex.

- Jerez Delgado, C. (2019). El daño moral en internet: en particular, la responsabilidad civil por la lesión de los derechos al honor, intimidad y propia imagen. En P. Escribano Tortajada y L. Martínez Vázquez de Castro (Dir.), *Internet y los derechos de la personalidad* (pp. 309-346). Tirant lo Blanch.
- López Richart, J. (2023). El Reglamento de Servicios Digitales: un nuevo marco de responsabilidad para los prestadores de servicios intermediarios en la Unión Europea. *Revista Aranzadi de Derecho y Nuevas Tecnologías* (62), 85-116.
- Mattace, G. (2024). La protección de los datos personales de los niños en el espacio digital, *Actualidad Jurídica Iberoamericana* (20), 1418-1438.
- Moliner Navarro, R. (2007). El derecho al honor y su conflicto con la libertad de expresión y el derecho a la información. En J. R. de Verda y Beamonte (Coord.), *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (pp. 21-53). Aranzadi.
- Moreno Martínez, J. A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. En J. Ataz López, J. A. Cobacho Gómez (Coords.), *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón, Tomo III* (pp. 515-567). Thomson Reuters Aranzadi.
- Navas Sánchez, M. M. (2017). El derecho a la propia imagen de los personajes públicos en las jurisprudencias constitucional, ordinaria y europea. Evolución concordancias y divergencias. *Revista de Derecho Político* (100), 441-480.
- Presno Linera, M. A. (2022). *Derechos fundamentales e inteligencia artificial*. Marcial Pons.
- Roselló Manzano, R. (2011). *Derechos de la personalidad y derechos morales de los autores*. Editorial Reus.
- Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución* (34), 197-232.
- Simó Soler, E. (2023) Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho. *InDret. Revista para el análisis del Derecho* (2), 1-23.
- Trujillo Cabrera, C. (2024). El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial. *InDret. Revista para el análisis del Derecho* (1), 74-113.
- Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Review* (9), 39-52.
- Vega García, P. (2023). Protección y comercialización del derecho a la propia imagen del difunto ante la inteligencia artificial. En A. Arrébola Blanco (Dir.), *Retos del Derecho de sucesiones en el siglo XXI. Vol. II* (pp. 999-1024). Reus.
- Ysás Solanes, M. (2013). Derechos en la esfera moral. En M. C. Gete-Alonso y Calera (Dir.) y J. Solé Resina (Coord.), *Tratado de derecho de la persona física. Tomo II* (pp. 833-876). Civitas-Aranzadi.

Responsabilidad civil derivada de la adquisición y utilización de *wereables* y servicios digitales en materia de salud¹

PEDRO J. FEMENÍA LÓPEZ

*Catedrático de Derecho civil.
Universidad de Alicante*

Sumario: 1. PLANTEAMIENTO: DE LA *E-HEALTH* A LA AUTONOMÍA INDIVIDUAL EN LA GESTIÓN DE LA SALUD. 2. RESPONSABILIDAD DERIVADA DE LA COMPRA DEL BIEN O DE LA CONTRATACIÓN DEL CONTENIDO O SERVICIO. 2.1. Ámbito de aplicación. 2.2. Sujeto responsable. 2.3. Criterios de imputación. 2.3.1 *Responsabilidad derivada de la falta de conformidad con los requisitos subjetivos u objetivos del contrato.* 2.3.2. *Responsabilidad general por incumplimiento contractual.* 3.- LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE *WEREABLES* Y SERVICIOS DIGITALES EN MATERIA DE SALUD. 3.1 Ámbito de aplicación. 3.2 Sujetos responsables. 3.3. Criterios de imputación. 3.3.1. *Responsabilidad objetiva.* 3.3.2. *Responsabilidad subjetiva o por culpa.*

1. PLANTEAMIENTO: DE LA *E-HEALTH* A LA AUTONOMÍA INDIVIDUAL EN LA GESTIÓN DE LA SALUD

Los nuevos enfoques científicos y el auge de las tecnologías digitales han provocado en los últimos años un cambio social basado en la democratización

¹ Este trabajo se enmarca en el Proyecto I+D+i (Referencia: PID2020-116185GB-I00) del Ministerio de Ciencia e Innovación: “La irrupción de la inteligencia artificial en el Derecho de Daños y su adaptación a las nuevas tecnologías”, en calidad de co-investigador principal. Así mismo en el Proyecto I+D+i de Excelencia PROMETEO 2023 (Referencia CIPROM/2022/40) de la Consellería de Educación, Universidades y Empleo de la Generalitat Valenciana: “La nueva era de los algoritmos y la inteligencia artificial y su tutela jurídica-privada en el marco de la Unión Europea”.

del conocimiento y en el crecimiento de una sociedad cada vez más informada y que reivindica una mayor participación por parte de ciudadanos no expertos en la producción del conocimiento y en la innovación.

El ámbito de la salud no permanece ajeno a este fenómeno. De entrada, debe advertirse que la expresión «salud» se emplea no solo como sinónimo de «ausencia de enfermedades y afecciones», sino también como «estado de completo bienestar, físico, mental y social».

La denominada «salud digital» (*eHealth*)² se abre camino a grandes pasos en la sociedad, pudiendo ser definida como el *conjunto de servicios sanitarios prestados de forma telemática, empleando tecnologías de la información, de la comunicación y sistemas de inteligencia artificial, que son compatibles, interoperables³ y aplicables en el diagnóstico y tratamiento de enfermedades, así como en la mejora del bienestar físico y mental de las personas*.

Las soluciones digitales aplicadas a la salud y la asistencia sanitaria pueden cambiar radicalmente el modo en el que se prestan los servicios sanitarios y asistenciales a los pacientes⁴, en tanto que la digitalización puede favorecer la continuidad del servicio asistencial transfronterizo; pueden ayudar a promover la salud y prevenir los sistemas sanitarios y su transición hacia modelos asistenciales centrados en las necesidades de la población; pueden contribuir a aplicar los conocimientos científicos sobre los ciudadanos, evitando que se conviertan en pacientes; y son susceptibles de permitir un mejor uso de los datos sanitarios en estudios de investigación e innovación, con el fin de pro-

² En la Unión Europea se utiliza el término *eSalud (eHealth)* para referirse a «la aplicación de las TIC en todo el rango de funciones que afectan al sector salud. Se incluyen productos, sistemas y servicios cubriendo aplicaciones sanitarias tales como redes corporativas; historia clínica electrónica; servicios de telemedicina, y sistemas personales llevables, no sólo las aplicaciones basadas en Internet». http://ec.europa.eu/information_society/activities/health/whatis_ehealth/index_en.htm. Sobre ello, MONTEAGUDO PEÑA, J.L.: «La e-Salud en el marco de la Unión Europea. Aspectos organizativos, legislativos y operacionales», <https://clubgertech.com/2022/04/04/la-e-salud-en-el-marco-de-la-union-europea/>.

³ NAVAS NAVARRO, S.: «Salud electrónica e inteligencia artificial», en S. Navas Navarro (Dir.) *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid 19)*, Comares, Granada, 2021, p. 9.

⁴ En este sentido, se afirma que «el sector de la salud digital, por su carácter integrador y su capacidad para incorporar modelos de innovación social en sus desarrollos, se percibe como uno de los campos de utilización intensiva de las aplicaciones de Internet de las Cosas o IoT (acrónimo de Internet of Things), que permiten la comunicación entre los propios objetos y entre éstos y las personas, lo que supone un claro ejemplo de la interacción entre los dominios de la medicina y las TIC (acrónimo de Tecnologías de la Información y las Comunicaciones)». MUÑOZ CARREÑO, en MARCOS GARCÍA, M.D.; RAMOS GONZÁLEZ, V.: *La administración segura de medicamentos en los nuevos escenarios electromagnéticos de Internet de las cosas (IoT)*, Madrid, Instituto de Salud Carlos III, Unidad de Investigación en Telemedicina y e-salud, 2018, p. 5.

mover una sanidad personalizada, mejorar las intervenciones y conseguir sistemas de salud y asistencia social más eficaces⁵.

La Unión Europea ha jugado un papel fundamental impulsando la aplicación de las TIC en el ámbito de la salud, a través de diversos programas que vienen desarrollándose desde hace cuarenta años⁶ y que han derivado a principios del presente siglo en el primer Plan de acción sobre la salud electrónica, publicado en 2004, al que siguió el actual Plan 2012-2020, cuya finalidad es «disponer de sistemas y servicios de salud electrónica con alta participación de los usuarios, que hagan hincapié en la interoperabilidad y la integración de las nuevas tecnologías centradas en los pacientes»⁷.

Además, se ha desarrollado un marco regulatorio y legislativo dirigido a promover la atención sanitaria a través de las fronteras de los Estados miembros, fomentando la colaboración regional, el intercambio de datos sanitarios y la mayor eficiencia de los sistemas sanitarios nacionales. En este ámbito se inscribe la Directiva 2011/24/EU, de 9 de marzo de 2011, sobre la aplicación de los derechos de los pacientes a la sanidad transfronteriza⁸ que define la «asistencia sanitaria» como «los servicios relacionados con la salud prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios»⁹.

La aplicación de la tecnología a la asistencia sanitaria se centra básicamente en tres esferas¹⁰:

- La primera, en los profesionales sanitarios, integrando toda una serie de herramientas que tienen que ver con los sistemas de información clínica dirigidos al personal sanitario para ser manejados dentro de las instituciones para las que trabajan (sistemas digitales de diagnóstico, radiología, información farmacéutica).

⁵ Vid. “La transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital”. <https://www.cgcom.es/la-transformaci%C3%B3n-digital-de-la-sanidad-y-los-servicios-asistenciales-en-el-mercado-%C3%BAnico-digital>

⁶ Se citan, en este sentido, diversos proyectos de investigación y desarrollo tecnológico relacionados con aplicaciones de informática bajo el primer programa ESPRIT (1984-1988) y de aplicaciones de telecomunicaciones de banda ancha dentro del Programa RACE (1987-1992). Además, fueron importantes los estudios BICEPS, presentados en 1986, que condujeron a la Acción Exploratoria de Informática Avanzada en Medicina AIM (1989-1990), origen de una serie de programas ininterrumpidos de I+D+i, dentro de los sucesivos Programas Marco, hasta el Horizonte 2020. MONTEAGUDO PEÑA, J.L.: “La e-Salud en el marco...”, cit.

⁷ *Plan de Acción de Salud Electrónica 2012-2020*, https://www.cgcom.es/europa_al_dia/2014/413

⁸ *Diario Oficial de la Unión Europea*, de 4 de abril de 2011, N° L 88, pp. 45-65.

⁹ Cfr. art. 3.a) Directiva 2011/24/UE.

¹⁰ NAVAS NAVARRO, S.: “Salud electrónica...”, cit., pp. 10-12.

- La segunda, en los centros hospitalarios, comprende la integración electrónica de los sistemas de información, a través de la historia clínica digital, la prescripción de medicamentos vía electrónica o solicitud de certificados médicos electrónicos. (big data sanitario).
- La tercera esfera, es la que relaciona a las dos primeras con el usuario del servicio, y en ella se integrarían la telemedicina y la sanidad a distancia (*m-Health*) mediante el uso de *apps médicas*, *chatbots*, *wearables* o *inteligencia artificial*.

Llegamos así al concepto de *m-Health* basado en la implementación de servicios sanitarios digitales mediante aplicaciones o dispositivos móviles, entre los que se incluyen los siguientes:

- *Chatbot*: El chatbot se concibe como un «programa de IA que permite al usuario-paciente introducir, en una base de datos operada mediante algoritmos matemáticos, determinada sintomatología de paciente, obtenida mediante la ordenación de las sucesivas respuestas a preguntas formuladas de forma abierta o cerrada (*Si/No/A veces/Frecuentemente/Siempre*)»¹¹. En el ámbito sanitario se han desarrollado tres tipos de chatbots¹²:
 - o *Chatbots conversacionales*. Diseñados para resolver problemáticas estándares, adaptándose al contexto para responder a las necesidades del usuario. Existen diferentes tipos de madurez en este tipo de bots, que marcarán el grado de profundidad en sus conversaciones. Utilizan tecnología NLP (natural language processing) y NLU (natural language understanding) para llevar a cabo el autoaprendizaje y entender el lenguaje y las necesidades de las personas.
 - o *Chatbots informativos*. Diseñados para que los usuarios puedan obtener información relevante en formato pop-up, actualizaciones o noticias de última hora. Este tipo de bots ofrece información de manera automatizada, además de un servicio de atención personalizada.
 - o *Chatbots prescriptivos*. Diseñados para ofrecer soluciones terapéuticas y no solo para dar respuestas o instrucciones. En este

¹¹ LUQUIN BERGARECHE, R.: “Responsabilidad contractual por el uso de la IA en la prestación de servicios de telemedicina y aplicaciones de salud digital”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora), p. 27.

¹² “Applications of Chatbots Available for the Healthcare Sector”, *Healthcare Tech Outlook*, 28/05/2021 <https://www.healthcaretechoutlook.com/news/applications-of-chatbots-available-for-the-healthcare-sector-nid-2366.html>

ámbito, *chatbots* como *Sara*, *Wisa* o *Woebot* ya se utilizan como psicoterapeutas virtuales, ayudando en el tratamiento de problemas psicológicos como la ansiedad o la depresión. También *One Remission Cancer Chatbot* se utiliza en el ámbito oncológico para proporcionar consejos e información útil sobre el cáncer¹³.

- *Wearables*: smartphones, tablets y otros dispositivos móviles como pueden ser brazaletes, gafas, pulseras, calzado o vestido, en los cuales se incorpora, o se descarga, un programa informático específico que tiene una finalidad médico-sanitaria¹⁴ y que pueden no estar prescritos por un profesional sanitario¹⁵. Como caracteres esenciales de estos productos y servicios se señalan¹⁶, en primer lugar la *movilidad*, esto es, la disponibilidad personal, en cualquier lugar y momento, de los datos y servicios sobre la salud para el usuario; y, en segundo lugar la *conectividad*, ya que se suele aludir a «salud conectada» o *wireless health* para referirse a estos productos y servicios sanitarios que permiten controlar la frecuencia cardíaca, el nivel de glucosa en sangre, la presión arterial, la temperatura corporal, así como también mejorar el estilo de vida basado en algoritmos sobre distancia recorrida, horas de sueño, nivel de estrés, hábitos de alimentación etc.
- *Apps*: Entre la numerosa oferta de apps existentes, se encuentran las denominadas *ePatient*, las cuales son aplicaciones que pueden instalarse en cualquier dispositivo inteligente (ordenadores, móviles, tablets, relojes...) para ofrecer servicios relacionados con el cuidado

¹³ Sobre ello, EBERS, M.: “Terapia sin terapeutas?”, en LUQUIN BERGARECHE, R. (Dir.): *Servicios privados de telemedicina y Salud Digital: retos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2023, pp. 32 y ss.

¹⁴ NAVAS NAVARRO, S.: “Salud móvil”, en S. Navas Navarro (Dir.) *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid 19)*, Comares, Granada, 2021, pp. 53-54.

¹⁵ Así ocurre, por ejemplo, con su uso en el mundo del deporte y la salud. Según la consultora CSS Insight, las ganancias en el sector de wearables superarían los 25.000 millones de dólares en 2020, y más de la mitad del negocio corresponderá a artículos relacionados con el deporte. En este ámbito, los wearables destacan por su doble funcionalidad en el deporte profesional: análisis del rendimiento y prevención de lesiones. Así, ya se usan pequeños dispositivos, incorporados en la ropa, que esconden un mini GPS, un acelerómetro para medir paradas y arrancadas, un giroscopio que mide la flexión y torsión del cuerpo, y un microprocesador que recopila y analiza hasta 1.000 referencias de datos por segundo transmitiéndolos a una pantalla en tiempo real. Información que permite a entrenadores y personal médico monitorizar valores como el rendimiento muscular, la respuesta del corazón, el ritmo de la respiración, la resistencia o la estamina.

Buena parte de lesiones están directamente relacionadas con la fatiga, y el análisis de datos permite a los equipos profesionales saber en todo momento el estado de forma de un deportista y los niveles de carga física que podrían derivar en lesión si no se actúa a tiempo. <https://johancruyffinstitute.com/es/blog-es/los-wearables-triunfan-industria-del-deporte/#>

¹⁶ NAVAS NAVARRO, S.: “Salud móvil”, cit., p. 54.

del paciente. Si bien la mayoría de ellas están dirigidas al área de bienestar personal, controlando la dieta, el sueño o el ejercicio, sus funciones pueden abarcar también el seguimiento o prevención de enfermedades¹⁷, como ocurre con aquellas que detectan la producción de una arritmia¹⁸, o la epilepsia¹⁹.

- *Inteligencia Artificial (IA)*: La aplicación de la IA al ámbito de la *m-Health* se basa, fundamentalmente, en la combinación de un volumen sustancial de datos y la capacidad de aprendizaje insertada en *hardwares* u otros dispositivos electrónicos de uso individual. De esta forma, los productos o servicios dotados de IA tienen capacidad propia para, de conformidad con los datos suministrados, y de manera totalmente autónoma, procesar esa información y emitir una decisión, solución o respuesta.

En cuanto a su objeto, la *m-Health* comprende, por un lado, al hardware (dispositivo móvil de que se trate con conectividad inalámbrica) y, por otro lado, al software (el programa informático específico, al que se denomina app) y que puede estar vinculado a un determinado dispositivo de forma indi-

¹⁷ Según datos proporcionados por <https://ticsalutsocial.cat/es/transparencia/> en el año 2017 había 325.000 aplicaciones sanitarias (de salud, condición física y aplicaciones médicas) disponibles en los mercados oficiales. Además, Android ha avanzado a Apple en número de aplicaciones de salud disponibles, estimándose en más de 84.000 los editores de aplicaciones médicas que están desarrollando apps para el mercado de la salud y el bienestar.

¹⁸ “Qué es la salud digital y qué beneficios aporta tanto al paciente como al profesional”, <https://campussanofi.es/e-professionals/noticias/que-es-la-salud-digital-y-que-beneficios-aporta-tanto-al-paciente-como-al-profesional/> (noticia de 23 de julio de 2020).

¹⁹ En este ámbito destacan (<https://vivirconeepilepsia.es/apps-y-wearables-que-ayudan-a-controlar-la-epilepsia>):

- SeizAlarm: Se trata de una aplicación desarrollada por Greg Pabst para el wearable de Apple capaz de avisar si el usuario está sufriendo una crisis epiléptica. Su desarrollador la ideó después de que a él mismo le diagnosticaran epilepsia, con el objetivo de poder avisar a sus familiares cuando le sobrevenía una crisis. La app permite hacer una solicitud de ayuda de forma inmediata o con retraso, en el caso de que empiecen los síntomas, pero no se esté seguro de si va a ocurrir la crisis.

- Control Diario de Epilepsia: Diseñada por la Fundación Carlos Slim, esta app pretende contribuir a mejorar la calidad de vida a pacientes con epilepsia, ofreciendo herramientas para realizar una monitorización de la enfermedad. Además, incluye funcionalidades para notificar emergencias, registrar fecha y hora de las crisis, administración de medicamentos, grabación de videos y registro de información relevante para el médico.

- EpiWatch: Desarrollada por profesores de Neurología de la Universidad Johns Hopkins, esta aplicación forma parte de un estudio de investigación y se centra en la interoperabilidad, gamificación, autocuidado, participación de profesionales sanitarios, sencillez de uso y utilidad. EpiWatch permite a los epilépticos llevar un control de sus crisis y predecir las futuras utilizando el reloj de Apple para registrar el ritmo cardíaco, el movimiento del cuerpo...

- App Epilepsia DCA: Es una aplicación desarrollada por una alumna de la Universidad de Alicante (UA) que permite detectar ataques epilépticos nocturnos en niños con Daño Cerebral Adquirido (DCA).

soluble con él, o bien funcionar de forma independiente a través de su descarga en una app-store o proveedor de servicios.

Su implementación y desarrollo se basa en la gestión de un gran volumen de datos ofrecidos de forma voluntaria por los ciudadanos²⁰, en el desarrollo y auge de Internet y de los dispositivos móviles que nos dirigen hacia nuevas formas de crear redes digitales de salud, y en la creación de dispositivos digitales de monitorización que permiten gestionar esos datos y ponerlos a disposición del individuo.

Cuando el uso de dichos dispositivos y servicios digitales ha sido prescrito por un profesional de la medicina forma parte de la relación médico-paciente y a ella queda sometido²¹. En cambio, cuando no han sido prescritos o suministrados por un profesional de la salud, el uso de dispositivos o servicios digitales en materia de salud supone un incremento de la participación ciudadana en la gestión de la salud. Este nuevo rol de los individuos²² provoca sustanciales beneficios tales como el aumento de la información y la autonomía derivada de tener un mayor control sobre la salud, poniéndose un énfasis especial en el aumento de la autonomía por parte de los ciudadanos y pacientes a la hora de tomar decisiones importantes sobre su propia salud, en tanto que no solo cumple con los requisitos de autodeterminación, de autorrealización y de empoderamiento²³, condiciones fundamentales para un desarrollo hu-

²⁰ Sobre ello vid. MÉNDEZ GARCÍA, M. y RODA FAURA, M.: “Aproximación práctica al uso de las tecnologías big data en el sector salud”, *DS (Derecho y Salud)*, n° Extra 1, 2017 (Ejemplar dedicado al XXVI Congreso de Derecho Sanitario y Ciudadanía Europea: los retos), pp. 152 y ss.

²¹ No es objeto del presente trabajo el estudio de la relación médico-paciente basada en el uso de servicios de telemedicina o salud digital. Sobre ello puede consultarse: LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit.

²² En este sentido, la *Opinión número 29 sobre las implicaciones éticas de las nuevas tecnologías en salud y la participación ciudadana*, desarrollada por el Grupo Europeo de Ética de la Ciencia y las Nuevas Tecnologías, afirma que «el “giro participativo” (*participatory turn*) en la salud ofrece diversos roles a los ciudadanos, investigadores, partes interesadas, proveedores de datos e información, participantes en las investigaciones y usuarios de la salud. Este giro participativo no solo no abarca la recopilación de información y acciones de voluntariado en torno a compartir datos así como la participación de personas no expertas en investigaciones y análisis científicos, sino también propicia los esfuerzos de los grupos de interés, la contribución del público a la investigación y a su financiación, así como la formulación de políticas y su regulación. La participación de los ciudadanos se manifiesta en diferentes etapas del proceso, desde su intervención en el establecimiento de prioridades y su influencia en las decisiones de financiación hasta una participación más directa de ciudadanos y pacientes en el uso y la aplicación del conocimiento de carácter médico. Abarca tanto a personas activas e informadas que se involucran desde posiciones estratégicas, así como a aquellos que desconocen su contribución». Vid. www.bioeticayderecho.ub.edu/archivos/pdf/EGE_opinion-29.pdf, pp. 1-2.

²³ Se afirma, en este sentido, que estamos transitando de un modelo que reconoce el derecho a la autonomía decisoria en cada intervención sanitaria mediante la prestación del consentimiento informado a otro, que, dando un paso adelante, rotundo y cualitativamente diferente, empodera al paciente tanto en lo que se refiere al uso de medios digitales en la asistencia sanitaria (teleconsultas,

mano pleno, sino que también mejora los resultados médicos y la eficacia de la asistencia²⁴.

No obstante, este cambio de rol en el control de la salud por parte de los individuos está siendo mediatizado por dinámicas externas que incluyen a actores comerciales cuyo máximo interés es la obtención de beneficios económicos²⁵ derivados de animar a los ciudadanos a tomar la iniciativa en la gestión de su propia salud, por medio de dispositivos y productos digitales que fomentan la toma de decisiones.

Por ello, este proceso debe ir acompañado de un control ético²⁶ y jurídico que procure un equilibrio entre autonomía y responsabilidad y evite la transferencia de responsabilidades derivadas de la gestión de la salud al individuo particular, ya que, en última instancia, dicha transferencia de responsabilidad podría suponer una reducción de los estándares y de la calidad de la asistencia sanitaria²⁷. Este control jurídico se hace especialmente relevante cuando los destinatarios se encuentran en situaciones de especial vulnerabilidad, tal y como puede ocurrir con las personas que padecen una discapacidad y que, en reconocimiento de su dignidad y autonomía, puedan servirse de estos productos o servicios, pero necesiten de las correspondientes medidas de apoyo;

teleasistencia, auto-monitorización de variables) como al proceso de control de los datos de salud de que es titular. LUQUIN BERGARECHE, R.: "Responsabilidad contractual...", cit., p. 2.

²⁴ *Opinión número 29...*, cit., p. 6.

²⁵ El volumen de negocio del mercado de Telemedicina en 2020 se estima en 45.000 millones de euros y constituye un elemento clave de la Estrategia del Mercado Digital de la Unión Europea. MONTEAGUDO PEÑA, J.L.: "La e-Salud...", cit.

²⁶ El sector sanitario posee una criticidad que debe ser valorada a la hora de implantar cualquier solución de Inteligencia Artificial. Es decir, la dimensión ética tiene que ser parte integral de su desarrollo, pero también de su introducción y posterior seguimiento. "Inteligencia Artificial. Ética en Sanidad". *DigitalES*, febrero 2022, https://www.digitales.es/wp-content/uploads/2022/02/Informe_IA_Etica_en_Sanidad.pdf

²⁷ La Agencia Española de Medicamentos y Productos Sanitarios (Aemps) ha puesto en marcha un portal (NotificaPS) para que profesionales y pacientes puedan notificar los incidentes con productos sanitarios al Sistema de Vigilancia de Productos Sanitarios. Dicha notificación supone un elemento esencial gracias al cual la Aemps registra los incidentes comunicados con el fin de identificar cualquier problema o defecto relacionado con los productos sanitarios. <https://www.redaccionmedica.com/secciones/ministerio-sanidad/en-marcha-la-notificacion-electronica-de-incidentes-en-productos-sanitarios-7180>

Por su parte, la FDA (Food and Drug Administration) ha anunciado, a través de un comunicado, la redacción de un marco regulatorio que permita la incorporación de nuevos enfoques en su programa piloto de evaluación de dispositivos de salud digitales, pretendiendo asegurar que los pacientes tengan acceso a nuevos productos como software de inteligencia artificial o relojes inteligentes que pueden ayudar a identificar una fibrilación auricular, que cumplan con los estándares de seguridad y eficacia. <https://www.redaccionmedica.com/secciones/tecnologia/estados-unidos-renueva-su-marco-de-evaluacion-en-salud-digital-6761>

o las personas mayores afectadas por la “brecha digital” y por la dependencia física y/o emocional de otras personas²⁸.

En el presente trabajo, analizaremos la responsabilidad civil derivada del uso de productos y servicios digitales en materia de salud, cuando dichos productos y servicios no forman parte de la relación médico-paciente, es decir, cuando no han sido prescritos o suministrados por un profesional de la medicina, pero se usan con una finalidad médico-sanitaria, tanto la que pueda resultar de la compraventa del bien o de la contratación del servicio digital, como aquella que derive del funcionamiento «defectuoso» o «normal» del producto, utilizando para ello el marco común de referencia proporcionado por las normas de la Unión Europea, así como las remisiones al Derecho interno que dichas normas realizan.

2. RESPONSABILIDAD DERIVADA DE LA COMPRA DEL BIEN O DE LA CONTRATACIÓN DEL CONTENIDO O SERVICIO

2.1. ÁMBITO DE APLICACIÓN

El primer supuesto de responsabilidad que podemos tratar en el ámbito de la utilización de productos o servicios digitales en materia de salud es el que deriva de la compra del bien o de la contratación del contenido o servicio digital.

Para dicho supuesto, resultan de aplicación, en primer lugar, dos Directivas del Parlamento Europeo y del Consejo dictadas ambas el 20 de mayo de 2019. La primera, es la Directiva 2019/770²⁹, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales; la segunda, es la Directiva 2019/771³⁰, relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modifican el Reglamento (CE) n° 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE³¹.

²⁸ Sobre la incidencia de la telemedicina en colectivos vulnerables vid., TORRELLES TORREA, E.: “Telemedicina y pacientes vulnerables”, en AA.VV.: *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, 2023, pp. 165 a 181.

²⁹ *Diario Oficial de la Unión Europea*, de 22 de mayo de 2019, N° L136, pp. 1- 27.

³⁰ *Diario Oficial de la Unión Europea*, de 22 de mayo de 2019, N° L136, pp. 28-50.

³¹ En relación a estas dos Directivas CÁMARA LAPUENTE ha destacado cuatro características especialmente relevantes: a) Se trata de normas “tecnológicamente neutras y que resisten el paso del tiempo” (*future-proof*); b) Se adopta el enfoque de la *armonización plena o de máximos*, con mínimas concesiones a la posibilidad de los Estados miembros de regular y elevar el nivel de protección de las Directivas; c)

Ambas, han sido incorporadas a nuestro ordenamiento por el Título VIII del Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores (BOE n° 101, de 28 de abril de 2021). El legislador español ha optado por su transposición mediante la modificación del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (BOE n° 287, de 30 de noviembre de 2007, en adelante *TRLGDCU*), adaptando el régimen actual a las novedades de las citadas normas europeas, cuya entrada en vigor se produjo el 1 de enero de 2022.

En orden a delimitar el ámbito de aplicación de cada una de ellas, es fundamental tener presente la distinción entre «bienes con elementos digitales incorporados o interconectados con ellos», siendo indiferente que el contenido o servicio digital esté preinstalado en el propio bien o que tenga que descargarse posteriormente³², a los que resultaría de aplicación la Directiva 2019/771, y «contenidos o servicios digitales independientes de los bienes a los que se incorporan», a los que resultaría de aplicación la Directiva 2019/770³³.

El concepto de «bienes con elementos digitales» debe referirse a bienes que incorporen «contenidos» o «servicios digitales» o estén interconectados con ellos de tal manera que la ausencia de dicho contenido o servicio digital

Sin embargo, *no se proponen reglas omnicomprendivas sobre todos los aspectos* de los contratos de suministro o compraventa, sino sólo una serie de reglas imperativas centradas en los problemas más destacados con los que se enfrentan los consumidores en estas relaciones jurídicas; se opta, en definitiva, por una armonización plena selectiva (*targeted full harmonisation*); d) Las reglas del contrato de suministro de contenidos y servicios digitales se basan en las diseñadas sobre la conformidad de los bienes con el contrato de compraventa, de manera que sólo se modulan para cubrir los rasgos genuinos de los contenidos digitales, de lo que deriva la decisión de presentar coetáneamente dos directivas distintas. Vid. CÁMARA LAPUENTE, S.: “El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015”, *InDret*, 3/2016, pp. 11 y 12.

³² JORQUÍ AZOFRA, M.: *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023, p. 153.

³³ Aunque ambas suponen importantes novedades en el ámbito de la defensa de los consumidores, se ha destacado que la Directiva 2019/770 consagra «por primera vez una regulación que unifica las legislaciones nacionales en materia de incumplimiento y remedios puestos a disposición del consumidor de contenidos y servicios digitales, con el fin de lograr un alto nivel de protección de los consumidores, reforzar la seguridad jurídica y, en definitiva, impulsar el denominado Mercado único Digital». SÁNCHEZ LERÍA, R.: “Mercado digital y protección del consumidor: a propósito de la Directiva 770/2019 y su transposición al ordenamiento jurídico español”, *InDret*, 4/2021, p. 36.

impediría que los bienes cumpliesen su función y en los que el contenido o servicio digital se facilita con los bienes en virtud de un contrato de compraventa relativo a esos bienes³⁴.

Por su parte, los conceptos de «contenido digital» y «servicio digital» vienen proporcionados por las Directivas 2019/770³⁵ y 2019/771³⁶ en los siguientes términos: el contenido digital lo constituyen «los datos producidos y suministrados en formato digital», por ejemplo, vídeo, audio, aplicaciones, juegos digitales y otro tipo de *software*, mientras que el servicio digital se define como «a) un servicio que permite al consumidor crear, tratar, almacenar o consultar datos en formato digital, o b) un servicio que permite compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos»³⁷, lo que permite la consideración de los sistemas de IA como contenido y/o servicio digital y, en consecuencia como «producto», a los efectos de la responsabilidad del fabricante de los mismos³⁸.

Para que los contenidos o servicios digitales incorporados o interconectados se consideren dentro del ámbito de aplicación de la Directiva 2019/771, y no de la Directiva 2019/770 son precisas dos condiciones³⁹: en primer lugar, que la ausencia de dichos contenidos o servicios digitales impida al bien cumplir su función; en segundo lugar, que esos elementos digitales se suministren con los bienes «con arreglo al contrato de compraventa», con independencia de que sean suministrados por el vendedor o por un tercero⁴⁰.

En relación a la tipología contractual, se ha afirmado en la doctrina que la pluralidad objetiva incide o puede llegar a incidir en la misma, especialmente en aquellos supuestos en los que las distintas prestaciones no comparten una misma naturaleza, proponiéndose la distinción entre una «pluralidad objetiva simple», que apelaría a la hipótesis de una prestación plural pero uniforme (como ocurriría en la compraventa de una pluralidad de bienes o en la contratación de una pluralidad de elementos digitales); y una «pluralidad objetiva compleja», que aludiría a los supuestos en los que el objeto contractual implica una mezcla de prestaciones de distinta naturaleza (como ocurriría en el negocio simultáneo de compraventa de bienes y contratación de servicios,

³⁴ Directiva 2019/770, considerando 21; y Directiva 2019/771, considerando 15.

³⁵ Arts 2.1 y 2.2.

³⁶ Arts. 2.6 y 2.7.

³⁷ Concepto que ha sido reproducido por el art. 59 bis TRLGDCU en sus apartados d) y o) respectivamente.

³⁸ JORQUÍ AZOFRA, M.: *Responsabilidad por los daños...*, cit., p. 154.

³⁹ JORQUÍ AZOFRA, M.: *Responsabilidad por los daños...*, loc. cit.

⁴⁰ Cfr. art. 3.3. Directiva 2019/771.

digitales o no, o en la contratación de servicios digitales y, a la vez, de servicios de otra índole o naturaleza)⁴¹.

En el supuesto que nos ocupa, el contrato recaerá sobre bienes o servicios de naturaleza mixta, es decir sobre «bienes con elementos digitales»⁴², o sobre «bienes formados por un elemento tangible que cumple funcionalmente el único cometido de servir de portador del contenido digital», habiendo optado el legislador europeo por trascender de aquella naturaleza mixta, reconduciendo íntegramente el bien a un único régimen aplicable, la Directiva 219/771 (art. 3.3), en el primer supuesto, y la Directiva 2019/770 (arts. 3.3 y 3.4,a), en el segundo⁴³.

El hecho de que el suministro del contenido o servicio digital incorporado o interconectado de forma permanente con el bien, forme o no parte del contrato de compraventa con el vendedor, es una cuestión interpretativa que dependerá del contenido de dicho contrato y será aplicable tanto a contenidos o servicios digitales incorporados o interconectados cuyo suministro se requiera expresamente en el contrato, como a contenidos o servicios digitales específicos que, a pesar de no estar requeridos expresamente en el contrato de compraventa, estén normalmente incluidos en bienes del mismo tipo y el consumidor pueda esperar razonablemente que lo estén dada la naturaleza de los bienes y teniendo en cuenta toda la declaración pública realizada por el vendedor o por su cuenta⁴⁴, o por otras personas en fases previas de la cadena de transacciones incluido el productor⁴⁵. Así, por ejemplo, en el supuesto de los relojes o pulseras inteligentes, con aplicaciones de salud, el propio reloj es el bien con elementos digitales, que únicamente podrá cumplir sus funciones con una aplicación que se suministra en virtud del contrato de compraventa y que el comprador debe descargar en un teléfono inteligente: la aplicación constituye, de esta forma, el elemento digital interconectado. De igual forma aplicaríamos este concepto de incorporación o interconexión a contenidos o servicios digitales que no son suminis-

⁴¹ ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad en contratos de compraventa y de suministro de elementos digitales con varias prestaciones”, *Cuadernos de Derecho Transnacional* (Marzo 2020), Vol. 12, N° 1, p. 797.

⁴² Art. 2.3 Directiva 2019/770; art. 2.5, b) Directiva 2019/771. Se han manifestado dudas, no obstante, sobre si determinadas funciones de los relojes de pulsera inteligentes estarían comprendidas en la noción de «contenidos digitales insertados en bienes de forma que operen como parte integrante de los mismos, o si, por el contrario, estarían excluidas del ámbito de aplicación por referencia expresa a la exclusión del denominado «internet de las cosas». En este sentido, CÁMARA LAPUENTE, S.: “El régimen de la falta de conformidad...”, cit., p. 15.

⁴³ ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad...”, cit., p. 798.

⁴⁴ Así ocurriría, por ejemplo, con versiones de wearables que, en declaración pública del fabricante o del vendedor, dicen incluir mejoradas todas las funciones de la versión anterior.

⁴⁵ Cfr. Directiva 2019/771, considerando 15.

trados por el propio vendedor, sino por un tercero en virtud del contrato de compraventa.

Por el contrario, si la ausencia de contenidos o servicios digitales incorporados o interconectados no impide que los bienes realicen sus funciones, o si el consumidor celebra un contrato cuyo objeto es el suministro de contenidos o servicios digitales que no forma parte de un contrato de compraventa de bienes con elementos digitales, estaríamos ante un contrato de suministro de elementos digitales que debe considerarse independiente del contrato de compraventa de los bienes, aunque el vendedor actúe como intermediario de ese segundo contrato⁴⁶. Así ocurre, por ejemplo, cuando el consumidor descarga en un teléfono inteligente o en un smartwatch una aplicación de salud, desde la tienda de aplicaciones⁴⁷.

En relación a los contenidos o servicios digitales en materia de salud, resulta, así mismo, fundamental, como hemos dicho, a la hora de delimitar la normativa aplicable, el hecho de que dicho «producto sanitario» no haya sido prescrito o suministrado por un profesional de la salud, ya que la Directiva 2019/770 únicamente resulta aplicable a contenidos o servicios digitales que constituyan productos sanitarios pero que el consumidor pueda obtener sin que sea prescrito o suministrado por un profesional de la salud, como ocurre por ejemplo con las aplicaciones sanitarias descargables de una app-store⁴⁸, disposición que ha sido incorporada al art. 114.e) del TRLGDCU.

Además, el ámbito de aplicación del contrato de suministro de contenidos o servicios digitales no depende del pago de un precio por los mismos, sino que también es extensible a aquellos modelos de negocio en los que el consumidor no paga un precio, pero facilita datos personales al empresario⁴⁹.

⁴⁶ No obstante, aspectos como la facultad de desistir del contrato, o el tiempo de la obligación de suministrar el contenido digital, quedarían al margen del contrato de suministro y pasarían a regularse por las reglas establecidas en la Directiva 2011/83, del Parlamento y del Consejo, de 25 de octubre, *sobre derechos de los consumidores*, según la redacción dada por el art. 2 (1) b de la Directiva 2019/2161, del Parlamento y del Consejo, de 27 de noviembre de 2019, *por la que se modifican la Directiva 93/13/CEE, del Consejo, de 5 de abril, la Directiva 98/6/CE, del Parlamento Europeo y del Consejo, la Directiva 2005/29/CE, del Parlamento Europeo y del Consejo y la Directiva 2011/83/UE, del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la UE*, sin que el contrato de suministro de contenidos digitales encuentre cabida, de momento, en la divergencia entre el contrato de compraventa (art. 2.5 Dir. 2022/83) y contrato de prestación de servicios (art. 2.6 Dir. 2011/83). Sobre ello, ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad...”, cit., p. 798.

⁴⁷ Cfr. Directiva 2019/770, considerando 22 y Directiva 2019/771, considerando 16.

⁴⁸ Cfr. Directiva 2019/770, considerando 29.

⁴⁹ Supuesto que ha quedado incorporado en el art. 59.4 TRLGDCU. Así ocurre, por ejemplo, en aquellos casos en que el consumidor abre una cuenta en una red social y facilita un nombre y una dirección de correo electrónico, y estos se utilizan para fines que no sean exclusivamente el suministro de los contenidos o servicios digitales, o distintos del cumplimiento de los requisitos legales; o en

En este sentido, además de reconocerse que la protección de datos personales es un derecho fundamental, por lo que estos no pueden ser considerados como un medio de pago, debe garantizarse que los consumidores, en el contexto de dichos modelos de negocio, tengan derecho a medidas correctoras contractuales derivadas del incumplimiento del empresario⁵⁰, así como a su derecho a retirar el consentimiento u oponerse al tratamiento de sus datos personales⁵¹.

En cambio, el pago de un precio es absolutamente necesario, en aquellos supuestos en los que el empresario recaba datos personales exclusivamente para suministrar contenidos o servicios digitales, o con el único fin de cumplir requisitos legales, tal y como ocurre en aquellos casos en los que el registro del consumidor es necesario en virtud de la legislación aplicable por motivos de seguridad e identificación⁵².

2.2. SUJETO RESPONSABLE

El sujeto responsable viene delimitado por el tipo de contrato que se celebre, ya sea de compraventa del bien que incorpora el elemento digital, o está interconectado con el mismo, ya se trate de un contrato de suministro de contenidos y servicios digitales no incorporados o interconectados con un bien concreto.

Cuando se trata de un contrato de compraventa, el art. 10 de la Directiva 2019/771, hace responsable al «vendedor», mientras que, si se trata de un contrato de suministro de contenidos y servicios digitales, el art. 9 de la Directiva 2019/770 hace responsable al «empresario». No obstante, se trata, en principio, de una cuestión meramente terminológica, ya que, a la hora de definir estos conceptos, ambas directivas optan por la misma fórmula: «toda persona física o jurídica, ya sea privada o pública, que actúa, incluso a través de otra persona que actúe en su nombre o por su cuenta, con un propósito relacionado con su actividad comercial, empresa, oficio o profesión, en relación con los contratos regulados por la presente Directiva»⁵³, concepto que es incorporado al art. 4 del TRLGDCU bajo la denominación de «empresario», añadiendo el art. 5 como «productor» al «fabricante del bien o al prestador del servicio

aquellos casos en que el consumidor dé su consentimiento para que cualquier material que constituya datos personales, como fotografías o mensajes que cargue, sea tratado por el empresario con fines comerciales.

⁵⁰ Cfr. Directiva 2019/770, considerando 24.

⁵¹ Cfr. art. 119 ter, apartado 7 TRLGDCU.

⁵² Cfr. Directiva 2019/770, considerando 25.

⁵³ Cfr. art. 2.3 Directiva 2019/771 y art. 2.5 Directiva 2019/770.

o su intermediario, o al importador del bien o servicio en el territorio de la Unión Europea, así como a cualquier persona que se presente como tal al indicar en el bien, ya sea en el envase, el envoltorio o cualquier otro elemento de protección o presentación, o servicio su nombre, marca u otro signo distintivo».

Así pues, el sujeto responsable viene definido por la actividad que se realiza y por el hecho de que dicha actividad forme parte del objeto del contrato, sin importar la condición de la persona, física o jurídica, su naturaleza, pública o privada, o el hecho de que actúe por cuenta propia o a través de otra persona que actúe en su nombre o por su cuenta. Así se pone de manifiesto claramente cuando se afirma que los «prestadores de plataformas» pueden ser considerados vendedores «si actúan con fines relacionados con sus propias actividades y en calidad de socio contractual directo del consumidor en la compraventa de bienes»⁵⁴.

2.3. CRITERIOS DE IMPUTACIÓN

A la hora de definir la responsabilidad derivada de la compraventa del bien o de la contratación del suministro de contenidos y servicios digitales, las Directivas y los arts. 115, bis, ter y quater del TRLGDCU regulan una responsabilidad especial derivada de la falta de adecuación de los bienes y/o de los contenidos o servicios contratados, con una serie de requisitos subjetivos y objetivos para la conformidad con el contrato, distinguiéndola de la responsabilidad general por incumplimiento contractual, cuya regulación se remite en las Directivas directamente al Derecho interno.

2.3.1. Responsabilidad derivada de la falta de conformidad con los requisitos subjetivos u objetivos del contrato

Con el fin de aportar claridad sobre lo que un consumidor puede razonablemente esperar de los bienes adquiridos o de los contenidos y servicios contratados, y delimitar la responsabilidad del vendedor o del empresario, se establecen unos «requisitos de conformidad» del contrato, tanto subjetivos como objetivos.

Los requisitos subjetivos para la conformidad⁵⁵ tienen que ver con la información suministrada al consumidor por parte del vendedor/empresario,

⁵⁴ Cfr. Directiva 2019/771, considerando 23.

⁵⁵ Cfr. art. 6 Directiva 2019/771; art. 7 Directiva 2019/770; art. 115 bis TRLGDCU.

relativos a la descripción, tipo, cantidad⁵⁶, calidad, funcionalidad, compatibilidad, interoperabilidad y demás características que disponga el contrato.

En relación a la cantidad y la calidad, su determinación se realizará en función de la naturaleza del contenido o servicio, no siendo posible, a priori, dar un concepto general de estos términos⁵⁷.

El concepto de funcionalidad se refiere a la forma en que los bienes, contenidos o servicios digitales realizan sus funciones teniendo en cuenta su finalidad, definiéndose en el TRLGDCU como «la capacidad de los contenidos o servicios digitales de realizar sus funciones teniendo en cuenta su finalidad»⁵⁸.

En cuanto a la compatibilidad, se define como la capacidad de los contenidos o servicios digitales de funcionar con los aparatos (hardware) o programas (software) con los cuales se utilizan normalmente los contenidos o servicios digitales del mismo tipo, sin necesidad de convertir los contenidos o servicios digitales⁵⁹.

Por su parte, el concepto de interoperabilidad hace referencia a la posibilidad que tienen los bienes de funcionar con aparatos (*hardware*) o programas (*software*) distintos de aquellos con los cuales se utilizan normalmente los bienes del mismo tipo⁶⁰. El buen funcionamiento podría incluir, por ejemplo, la capacidad de los bienes para intercambiar información con esos otros programas o aparatos y utilizar la información intercambiada⁶¹.

De igual forma, los requisitos subjetivos afectan a la información suministrada al consumidor relativa a los accesorios, instrucciones, asistencia al consumidor y actualizaciones, según disponga el contrato.

Especial consideración merecen, en este sentido, las actualizaciones, ya que pueden mejorar y reforzar los contenidos o servicios digitales, individual-

⁵⁶ No ha resultado, sin embargo, unánime en la doctrina la interpretación de la cantidad como criterio de conformidad en los trabajos anteriores a las Directivas de 2019. A favor de considerar la entrega parcial como un supuesto de falta de conformidad se muestran CARRASCO PERERA, A.; CORDERO LOBATO, E.; MARTÍNEZ ESPÍN, P.: “Transposición de la Directiva comunitaria sobre venta y garantías de los bienes de consumo”, *Estudios sobre consumo*, n.º 52, 2000, p. 127. Por el contrario, sostienen que a falta de previsión expresa de la cantidad como criterio de conformidad en la legislación nacional, debe acudir a las normas internas sobre incumplimiento contractual MARTÍNEZ VELENCOSO, L.M.: *La falta de conformidad en la compraventa de bienes*, Bosch, Barcelona, 2007, p. 77. Tras la entrada en vigor de las Directivas de 2019, expresamente, ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad...”, cit., p. 799.

⁵⁷ SÁNCHEZ LERÍA, R.: “Mercado digital y protección del consumidor...”, cit., p. 54.

⁵⁸ Art. 59 bis l).

⁵⁹ Art. 59 bis c) TRLGDCU.

⁶⁰ Art. 59 bis ñ) TRLGDCU.

⁶¹ Cfr. Directiva 2019/771, considerando 27.

mente considerados o incorporados a un bien, ampliar sus funcionalidades, adaptarlos a los avances técnicos, protegerlos frente a las nuevas amenazas para la seguridad⁶² o servir a otros fines. Por ello, se consideran parte integrante del bien, contenido o servicio digital de manera que la conformidad de los mismos también debe evaluarse en función de si la actualización se ha prestado en la forma estipulada en el contrato. La falta de suministro de actualizaciones acordadas en el contrato, se considerará una falta de conformidad de los bienes, contenidos o servicios digitales. Además, las actualizaciones defectuosas o incompletas también serán consideradas una falta de conformidad con los requisitos subjetivos del contrato⁶³.

No obstante, la obligación del vendedor/empresario en relación a las actualizaciones se limita a aquellas necesarias para que los bienes, contenidos o servicios mantengan su adecuación con los requisitos de conformidad subjetivos y objetivos del contrato. De esta forma, salvo que estuviera expresamente pactado en el contrato, el vendedor/empresario no está obligado a proporcionar al consumidor versiones mejoradas de los contenidos o servicios digitales, ni a mejorar o ampliar sus funcionalidades más allá de los requisitos de conformidad⁶⁴.

En última instancia, corresponde siempre al consumidor la libertad de elegir si instala o no las actualizaciones facilitadas. La decisión de no instalar las actualizaciones, cuando estas son necesarias para mantener la conformidad de los bienes, contenidos o servicios contratados, actuará como causa de exclusión de la responsabilidad del vendedor/empresario por falta de conformidad, si bien el propio vendedor/empresario está obligado a informar al consumidor de esta circunstancia⁶⁵.

Por el contrario, los requisitos objetivos para la conformidad⁶⁶ tienen que ver con las cualidades y características de los bienes adquiridos o de los contenidos y servicios contratados, considerando, entre otros factores, el fin para el que se utilizarían normalmente los bienes, contenidos o servicios contratados, si se suministran con los accesorios e instrucciones o versión de prueba que el consumidor puede esperar razonablemente recibir, o si corresponden a la muestra o modelo que el vendedor facilitó al consumidor⁶⁷.

⁶² El vendedor/empresario también se obliga a facilitar actualizaciones de seguridad, con el fin de garantizar que los bienes, contenidos o servicios sigan siendo conformes. Cfr. Directiva 2019/771, considerando 30.

⁶³ Cfr. Directiva 2019/771, considerando 28.

⁶⁴ Cfr. Directiva 2019/771, considerando 30.

⁶⁵ Cfr. Directiva 2019/771, considerando 30.

⁶⁶ Cfr. art. 7 Directiva 2019/771; art. 8 Directiva 2019/770 y art. 115 ter TRLGDCU.

⁶⁷ Cfr. Directiva 2019/771, considerando 29.

A tenor del régimen jurídico establecido en las Directivas e incorporado al TRLGDCU, la responsabilidad derivada de la falta de conformidad con los requisitos subjetivos u objetivos del contrato es una responsabilidad cuasi objetiva, ya que, a pesar de estar basada en la culpa, se produce una inversión de la carga de la prueba a favor del destinatario del bien o del servicio, así como una presunción de culpabilidad durante un plazo de garantía.

Así, la Directiva 2019/771 dispone, en su considerando 42, que los Estados miembros deben tener la facultad de disponer que el vendedor sea responsable de toda falta de conformidad que se manifieste en un plazo de garantía determinado, plazo de garantía que habrá de combinarse con el plazo de prescripción para ejercer la acción, establecido por cada ordenamiento interno, de manera que se garantice que dicho plazo de prescripción no restrinja el derecho de los consumidores a exigir responsabilidad derivada de la falta de conformidad que se manifieste dentro del plazo de garantía. Esta disposición fue incorporada al art. 120 del TRLGDCU al disponerse, en su apartado, primero, que «en el caso de compraventa de bienes o de suministro de contenidos o servicios digitales suministrados en un acto único o en una serie de actos individuales, el empresario será responsable de las faltas de conformidad que existan en el momento de la entrega o del suministro y se manifiesten en un plazo de tres años desde la entrega en el caso de bienes o de dos años en el caso de contenidos o servicios digitales...». Por su parte, cuando el contrato prevé el suministro continuo de contenidos o servicios digitales durante un período de tiempo indeterminado, el apartado segundo del mismo precepto establece que «el empresario será responsable de cualquier falta de conformidad de los contenidos o servicios digitales que se produzca o se manifieste dentro del plazo durante el cual deben suministrarse los contenidos o servicios digitales de acuerdo con el contrato», si bien, si el contrato establece un período de suministro continuo inferior a tres años, «el plazo de responsabilidad será de tres años a partir del momento de la entrega».

En todo caso, salvo prueba en contrario, se presumirá que las faltas de conformidad que se manifiesten en los dos años siguientes a la entrega del bien o en el año siguiente al suministro del contenido o servicio digital suministrado en un acto único o en una serie de actos individuales, ya existían cuando el bien se entregó o el contenido o servicio digital se suministró⁶⁸.

La falta de conformidad se traduce en la responsabilidad del vendedor/empresario que permitirá al consumidor ejercer la acción de puesta en conformidad o cumplimiento forzoso del contrato⁶⁹, incluyendo la reparación

⁶⁸ Art. 121.1 TRLGDCU y Directiva 2019/771, considerando 45.

⁶⁹ Art. 118 TRLGDCU. Esta posibilidad debe también considerarse inserta en ambas directivas, a pesar de contemplarse únicamente de forma genérica en el art. 14 de la Directiva 2019/770.

o sustitución de los bienes salvo que las mismas resulten imposibles o impongan costes que resultarían desproporcionados⁷⁰; la acción *quantum minoris*, exigiendo una rebaja proporcional en el precio, cuando el vendedor se niegue o no lleve a efecto la reparación o sustitución, cuando no sea posible o, a pesar de la misma, subsista la falta de conformidad, o cuando la falta de conformidad sea de tal gravedad que se justifique la reducción inmediata del precio⁷¹; o, en última instancia, la acción resolutoria del contrato, cuando la falta de conformidad sea grave, con derecho a suspender los pagos pendientes⁷².

No obstante, en el caso de la compraventa de bienes, la propia Directiva 2019/771 establece que las medidas correctoras contempladas en la misma no afectan a la facultad de los Estados miembros de permitir a los consumidores elegir una medida correctora concreta si la falta de conformidad de los bienes se manifiesta poco después de la entrega, como serían las disposiciones nacionales que establezcan el derecho del consumidor a rechazar los bienes que presenten un vicio⁷³ y a considerar denunciado el contrato, o a pedir la sustitución inmediata del bien, dentro de un breve plazo no superior a treinta días después de la entrega⁷⁴.

Esta responsabilidad del empresario/vendedor es independiente de la indemnización, en concepto de daños y perjuicios, que puede reclamar el consumidor, indemnización que, por venir garantizada en el Derecho interno, coloca el régimen de responsabilidad de las Directivas en una esfera distinta e independiente de las normas nacionales sobre compensación de los consumi-

De otra forma, tendría difícil encaje la presentación de la cantidad como criterio de conformidad, con los remedios expresos previstos en el art. 13 de la Directiva 2019/771 (reparación y sustitución), ya que la puesta en conformidad de los bienes entregados solo parcialmente, se aviene únicamente con la acción dirigida a entregar la parte restante. ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad...”, cit., p. 801. En cualquier caso, en la doctrina ya se había propuesto una interpretación integradora favorable a considerar que la reclamación de la parte restante «equivale a solicitar la reparación». Así, ARROYO Y AMAYUELAS, E.: “La propuesta de Directiva...”, cit., pp. 9-10; o MARÍN LÓPEZ M.J.: “Comentario al art. 116”, en R. BERCOVITZ RODRIGUEZ-CANO (COORD.), *Comentario del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*, Thomson Reuters, Pamplona, 2009, p. 1442, para el cual la sustitución como medida reparadora deben entenderse «en el sentido de que debe reemplazarse la prestación ejecutada por la pactada en el contrato».

⁷⁰ Cfr. Art. 13 Directiva 2019/771; art. 14 Directiva 2019/770 y art. 118.3 TRLGDCU.

⁷¹ Cfr. Arts. 13.4 y art. 15 Directiva 2019/771 y arts. 119 y 119 bis TRLGDCU.

⁷² Cfr. Arts. 13.5 y 6, art. 16 Directiva 2019/771 y art. 119 ter TRLGDCU.

⁷³ Sobre esta cuestión, GSELL, B. Y RODRIGO ARALEDI, LL. M.: “Plazos de las medidas correctoras en caso de vicios ocultos según la Directiva (UE) 2019/770 sobre contratos de suministro de contenidos y servicios digitales y la Directiva (UE) 2019/771 sobre el contrato de compraventa de bienes”, *Cuadernos de Derecho Transnacional*, Octubre, 2020, vol. 12, n° 2, pp. 475 y ss.

⁷⁴ Cfr. Directiva 2019/771, considerando 19.

dores y usuarios por los daños y perjuicios que se deriven del incumplimiento de esas normas⁷⁵.

2.3.2. Responsabilidad general por incumplimiento contractual

La responsabilidad del vendedor/empresario por falta de conformidad con los requisitos subjetivos u objetivos del contrato es independiente de la responsabilidad general basada en cualquier otro incumplimiento contractual, la cual queda sometida al Derecho interno.

Así ocurre con la responsabilidad derivada de la legalidad de los bienes; aspectos generales de Derecho contractual como la celebración, validez, nulidad o efectos de los contratos; o la responsabilidad derivada de vicios que no fueran manifiestos en el momento en que se celebró el contrato de compra-venta, sometidas a los correspondientes preceptos de nuestro Código civil.

Además, el destinatario de estos servicios puede beneficiarse de la aplicación de las normas del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU), en lo referente a la regulación de cláusulas abusivas, responsabilidad por productos o servicios defectuosos, publicidad del contrato, garantías y servicios posventa, etc., siempre y cuando los servicios no hayan sido prestados directamente por un profesional sanitario⁷⁶. Así se deduce del art. 93.b) TRLGDCU que excluye del ámbito de aplicación del Título III (Contratos celebrados a distancia y contratos celebrados fuera de establecimiento mercantil) a “*los contratos de servicios relacionados con la salud, prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios, con independencia de que estos servicios se presten en instalaciones sanitarias*”.

De igual forma, el art. 66 bis TRLGDCU, relativo a la obligación de entrega en plazo y la posibilidad de resolución del contrato, no se aplica a los contratos excluidos de las normas sobre contratos a distancia como los servicios sanitarios; o el art. 114 TRLGDCU, relativo a garantías y servicios posventa, que excluye de su ámbito de aplicación “*los contenidos o servicios digitales relacionados con la salud prescritos o suministrados por un profesional sanitario a pacientes*”.

⁷⁵ Cfr. Directiva 2019/771, considerando 61.

⁷⁶ La exclusión, cuando dichos servicios se prestan directamente por profesionales sanitarios, se basa en que la asistencia sanitaria exige una regulación especial debido a su complejidad técnica, su importancia como servicio de interés general y, en su caso, su financiación pública. LUQUIN BERGARECHE, R.: “Responsabilidad...”, cit., p. 8.

para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios”.

3. LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE *WEAREABLES* Y SERVICIOS DIGITALES EN MATERIA DE SALUD

El segundo supuesto que debe analizarse es el de la responsabilidad derivada del uso de estos productos y aplicaciones digitales en materia de salud, supuesto que adquiere un grado de complejidad mucho mayor dada la posible confluencia de varias normas en la delimitación del régimen de responsabilidad aplicable.

Surge, en primer lugar, la duda de si tales productos y servicios digitales pueden ser calificados como «productos sanitarios», puesto que dicha calificación incide directamente en su régimen jurídico. La regulación de los productos sanitarios se contiene en el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017, sobre los productos sanitarios⁷⁷ (RPS), por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) num. 178/2002 y el Reglamento (CE) num 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo, relativa a los productos sanitarios⁷⁸. Aunque el RPS resulta de aplicación directa en los países de la Unión Europea, era necesario regular, a nivel nacional, los aspectos que el propio reglamento remite a dicha regulación, razón por la cual se aprobó en España el Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios⁷⁹ y en el que se regulan cuestiones como la determinación de la autoridad competente a efectos del reglamento, el régimen de garantías sanitarias de los productos, la fijación del régimen lingüístico, o la regulación de los procedimientos para la fabricación de productos para su uso en el propio centro sanitario y para el reprocesamiento de productos de un solo uso y su utilización.

Pero, además, debe tenerse en cuenta la capacidad de algunos de estos dispositivos para aprender por sí mismos, derivada de la programación con sistemas de inteligencia artificial, supuesto que no está contemplado

⁷⁷ *Diario Oficial de la Unión Europea*, de 5 de mayo de 2017, N° L117, pp. 1-34.

⁷⁸ *Diario Oficial de las Comunidades Europeas*, de 12 de julio de 1993, N° L169, pp. 1-43, recogido anteriormente en la Directiva 90/385/CEE del Consejo, de 20 de junio de 1990, relativa a la aproximación de las legislaciones de los Estados miembros sobre los productos sanitarios implantables activos (*Diario Oficial de las Comunidades Europeas*, de 20 de julio de 1990, N° L189, p. 17) y posteriormente en la Directiva 98/79/CE del Parlamento Europeo y del Consejo, de 27 de octubre de 1998, sobre productos sanitarios para diagnóstico in vitro (*Diario Oficial de las Comunidades Europeas*, de 7 de diciembre de 1998, N° L331, p. 1).

⁷⁹ BOE n° 69, de 22 de marzo de 2023.

en el RPS y para el que deberíamos acudir al *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre Inteligencia Artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)*, conocido comúnmente como Ley de Inteligencia Artificial (RLIA)⁸⁰, publicado en el Diario Oficial de la Unión Europea el 12 de julio de 2024⁸¹ y cuyo régimen de responsabilidad se desarrolla en la Propuesta de Directiva del Parlamento Europeo y del Consejo, de 28 de septiembre de 2022, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (PDRIA)⁸², que todavía no ha entrado en vigor.

Por si fuera poco, el carácter de bienes de consumo de los productos o servicios a los que nos referimos hace posible la aplicación de la legislación en materia de responsabilidad derivada de productos defectuosos, constituida en nuestro caso por el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU)⁸³, cuyo artículo 136 limita el concepto legal de producto a «cualquier bien mueble, aun cuando esté unido o incorporado a otro bien mueble o inmueble, así como el gas y la electricidad».

No obstante, la normativa europea actual sobre responsabilidad por daños causados por productos defectuosos⁸⁴ ha devenido obsoleta en tanto que no queda claro cómo aplicarla a los productos de la economía digital moderna, como los programas informáticos y los productos que necesitan programas o servicios digitales para funcionar, en especial a la inteligencia artificial y, además, la aparición y desarrollo de dichos productos plantea dificultades

⁸⁰ Su «objetivo primordial es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea...». Cfr. RLIA. Considerando (1).

⁸¹ https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689

⁸² Bruselas 28.9.2022, COM (2022) 496 final, 2022/0303 (COD), <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496>, (Fecha consulta 13.02.2024).

⁸³ BOE de 30 de noviembre de 2007.

⁸⁴ Directiva 85/374/CEE, del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, DOCE n° 210, de 7 de agosto de 1985, pp. 29 a 33.

probatorias para los perjudicados en “casos complejos” desde un punto de vista técnico y científico⁸⁵.

Al objeto de superar estos problemas, la Comisión Europea publicó, también el 28 de septiembre de 2022, la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos⁸⁶, aprobada por Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024 (DRPD)⁸⁷, cuyo objeto principal es solventar las «dificultades para obtener una indemnización debido a restricciones a la hora de presentar reclamaciones de indemnización y a las dificultades a la hora de reunir pruebas para demostrar la responsabilidad, especialmente a la luz de la creciente complejidad técnica y científica (...) Por lo tanto, la revisión fomentará la implantación y aceptación de esas nuevas tecnologías, incluida la IA, garantizando al mismo tiempo que los demandantes puedan disfrutar del mismo nivel de protección con independencia de la tecnología de que se trate y que todas las empresas se beneficien de más seguridad jurídica y de unas condiciones de competencia equitativas⁸⁸.

3.1. ÁMBITO DE APLICACIÓN

La calificación como «productos» de los bienes y servicios digitales que integran la denominada *M-Health*, y a los que venimos haciendo referencia en el presente trabajo está fuera de toda duda.

⁸⁵ Ya en su Informe de evaluación de la Directiva de Productos Defectuosos, la Comisión Europea advirtió en 2018 que «los problemas a los que nos enfrentamos en la actualidad difieren en cierta medida de los que existían en el mundo predominantemente analógico de 1985. Nos encontramos inmersos en otra revolución tecnológica. La economía y los propios productos están aumentando gradualmente su interconexión, su digitalización, su autonomía y su inteligencia. Necesitamos una respuesta coherente y global ante estos retos, tal como se describe en la iniciativa sobre inteligencia artificial». Vid. *Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre la aplicación de la Directiva del Consejo relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85/374/CEE)*, Bruselas 7.5.2018, COM (2018) 246 final, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0246&from=FR> (fecha consulta 13.02.2024), p. 9.

⁸⁶ Bruselas 28 de septiembre de 2022, COM (2022) 495 final; 2022/0302 (COD). <https://eur-lex.europa.eu/legal-content/ES/TXT/DOC/?uri=CELEX:52022PC0495> (Fecha consulta 13.02.2024). Un análisis de la misma en ATIENZA NAVARRO, M.L.: “¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)”, *Indret*, 2.2023.

⁸⁷ P9_TA(2024)0132 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.pdf (fecha de consulta 8 de mayo de 2024)

⁸⁸ Cfr. DRPD, Considerando (3).

Respecto de los bienes, por cuanto que, como señala la nueva DRPD en su considerando 13, los «productos» en la era digital pueden ser tangibles o intangibles. Los programas informáticos, como los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. En este sentido, los programas informáticos pueden ser considerados como productos en sí mismos, o como parte integrante de otros productos, es decir como componentes de los mismos. Así pues, los programas informáticos constituyen un «producto» con independencia de si están almacenados en un dispositivo, se accede a los mismos a través de una red de comunicaciones o tecnologías en la nube, o se suministra a través de un modelo de programa informático como servicio.

En relación a los servicios, cada vez es más frecuente que los servicios digitales se integren o estén interconectados con un producto, de tal manera que la ausencia del servicio impediría al producto desarrollar alguna de sus funciones. Por ello, la DRPD aplica la consideración de «componente de un producto» a estos servicios conexos cuando se integran el mismo o están interconectados con él bajo el control del fabricante de dicho producto, poniendo como ejemplo específico, entre otros, los servicios de vigilancia de la salud que se basan en sensores de un producto físico para rastrear la actividad física o los parámetros de salud del usuario⁸⁹.

También las actualizaciones y mejoras de programas informáticos se consideran «componentes» de un producto cuando están integrados en dicho producto o interconectados con él, y son suministrados por el fabricante, o cuando el fabricante consienta su integración, interconexión o suministro por parte de un tercero⁹⁰.

En cuanto a la calificación de estos bienes y servicios como «productos sanitarios», el concepto de los mismos se contiene en el art. 2.1 RPS que considera como tales cualquier instrumento, dispositivo, equipo, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos, que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de: diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad; diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad; investigación, sustitución, o modificación de la anatomía o de un proceso o estado fisiológico o patológico; regulación de la concepción, obtención de información mediante el examen *in vitro* de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos;

⁸⁹ Cfr. DRPD, considerando 17.

⁹⁰ Cfr. DRPD, considerando 18.

y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios.

Por su parte, el art. 6 del RPS extiende la consideración de «producto sanitario» a los ofrecidos a través de la sociedad de la información, incluso a los productos no introducidos en el mercado, pero utilizados en el contexto de una actividad comercial, bien sea de forma remunerada o gratuita, para prestar un servicio diagnóstico o terapéutico a través de servicios de la sociedad de la información, o de otros medios de comunicación, directamente o a través de intermediarios.

A estos efectos, se señalan en la doctrina⁹¹ dos factores decisivos para la calificación de los productos sanitarios: que el producto tenga una finalidad *prevista* y que dicha finalidad sea *médica*. La finalidad *prevista* se desprende del etiquetado, las instrucciones de uso o el material publicitario suministrado por el fabricante, por lo que la forma en la que el fabricante anuncia y describe el producto puede tener una incidencia decisiva en su calificación como producto sanitario. Así, se dice que un brazalete por medio del cual se monitoriza la frecuencia cardiaca de la persona puede quedar fuera de la consideración de «producto sanitario», si el control de la frecuencia cardiaca no sirve para ninguna finalidad médica, estando destinado únicamente a proporcionar información al usuario mientras realiza ejercicio físico⁹². En relación a este factor, debe tenerse en cuenta, por tanto, que un producto puede tener más de una finalidad prevista, por lo que se añade que alguna de esas finalidades sea *médica* para que el producto pueda ser calificado como sanitario⁹³.

Sobre la interpretación de este concepto se pronunció el TJUE, en su sentencia de 22 de noviembre de 2012, caso *Brain Products GmbH c. BioSemi VOF y otros*⁹⁴,

⁹¹ LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit., pp. 33-34.

⁹² ALKORTA IDIAKEZ, I.: *El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Aranzadi, Pamplona, 2022, p. 80.

⁹³ A tenor del art. 1(3) RPS «Los productos que tengan tanto finalidad médica como no médica deberán cumplir de forma acumulativa los requisitos aplicables a los productos con finalidad médica y las aplicables a los productos sin finalidad médica».

⁹⁴ ECLI:EU:C:2012:742. Vid. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62011CJ0219> (Fecha consulta 20.02.2024). Dicha sentencia resuelve una petición de decisión prejudicial planteada en el marco de un litigio entre «Brain Products» frente a «Biosemi y otros», en relación con la aplicación de la Directiva 93/42 (precedente del actual RPS) a un producto, cuyo uso no médico había sido definido por su fabricante, destinado a fines de investigación de un proceso fisiológico. Biosemi y otros se dedicaban a la comercialización de sistemas y equipos electrónicos, en particular de un sistema que permite registrar la actividad cerebral humana denominado «Active Two». Según la sociedad alemana Brain Productos, dado que Active Two constituye un producto sanitario y que Biosemi y otros no disponían de certificación CE para tales productos, esa comercialización debía estar prohibida. Frente a ello, Biosemi y otros sostenían que, habida cuenta de que Active Two no estaba destinado a una finalidad médica, no podía calificarse como «producto

en la cual, al resolver la cuestión prejudicial sobre si la «finalidad médica» constituye o no un requisito implícito del concepto de «producto sanitario», parte de la consideración que, a este respecto, establece el legislador europeo respecto de los programas informáticos, al prever que, para que dichos programas informáticos queden comprendidos en el concepto de «producto sanitario», «...no basta con que se utilicen en un contexto sanitario, sino que es necesario que su finalidad definida por su fabricante, sea específicamente médica» (considerando 17), concluyendo que «el concepto de producto sanitario sólo cubre un objeto concebido por su fabricante para ser utilizado en seres humanos con fines de investigación de un proceso fisiológico, si se destina a fines médicos».

Como puede observarse, por tanto, el concepto de «producto sanitario» es, en principio, un concepto amplio que permite englobar en el mismo no sólo los productos concebidos exclusivamente con finalidad médica, sino aquellos otros que, habiendo sido concebidos con una finalidad distinta, sean destinados a fines médicos. Ello permitiría incluir aquellos dispositivos y servicios digitales utilizados solos, o en combinación con programas informáticos, destinados al seguimiento de funciones básicas para el funcionamiento normal del organismo y que inciden, por tanto, de manera directa en el tratamiento, predicción o pronóstico de una enfermedad.

De esta forma, tras la entrada en vigor del RPS, los dispositivos, prendas inteligentes o aplicaciones móviles que, entre otras funciones, estén destinadas por el fabricante para ser utilizadas en las personas, por separado o en combinación con otros productos, con algún fin médico específico como el diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad, podrían calificarse como productos sanitarios⁹⁵. Así ocurriría con la persona diabética que controla sus niveles de azúcar en sangre con su *smartphone*, o el individuo con riesgo de sufrir patologías del corazón que controla su frecuencia cardíaca, saturación de oxígeno en sangre o presión sanguínea a través de su reloj inteligente.

Es necesario precisar, en este sentido, que los programas informáticos por sí mismos, cuando están destinados específicamente por el fabricante a una o varias de las finalidades médicas establecidas en la definición de producto

sanitario», sosteniendo, además, que el hecho de que ese sistema pueda ser transformado en aparato de diagnóstico no supone que deba ser clasificado como «producto sanitario». En primera y segunda instancia los tribunales alemanes consideraron que no podía calificarse Active Two como «producto sanitario» toda vez que no cumplía el requisito adicional implícito a dicho concepto que es la «finalidad médica» del sistema. Planteado el recurso de casación, el *Bundesgerichtshof* albergó dudas sobre si la «finalidad médica» constituye o no un requisito adicional implícito del concepto de «producto sanitario», por lo que planteó la cuestión prejudicial ante el TJUE.

⁹⁵ LANDA REZA, I.: *El consentimiento de la persona mayor con discapacidad para el tratamiento de sus datos relativos a la salud*, Atelier, Barcelona, 2023, pp. 54-55.

sanitario, constituyen productos sanitarios⁹⁶, pero los programas informáticos para usos generales, aun cuando se utilicen en el marco de la asistencia sanitaria, o los programas informáticos destinados a objetivos de bienestar o estilo de vida, no son productos sanitarios, tal y como ocurriría con los *wereables* o aplicaciones en virtud de las cuales la persona adapta su régimen alimenticio y hábitos de vida en función de lo que dicta su reloj o pulsera inteligente.

Además, los productos ofrecidos a personas a través de la sociedad de la información y los utilizados en el contexto de una actividad comercial para prestar un servicio de diagnóstico o terapéutico a personas en el ámbito de la Unión Europea, deben cumplir también los requisitos del RPS, cuando el producto en cuestión se introduzca en el mercado o el servicio comience a prestarse en la Unión⁹⁷.

Desde este punto de vista, los *wereables*, las aplicaciones móviles o las plataformas digitales dedicadas a monitorizar la frecuencia cardiaca, el nivel de glucosa en sangre, o la presión arterial, que permiten un seguimiento de la enfermedad utilizando, por ejemplo, la generación de alarmas, podrían tener la consideración de «producto sanitario», mientras que aquéllas que pretenden monitorizar nuestro estilo de vida, a través de patrones como el número de pasos, las calorías consumidas o las horas de sueño, no entrarían dentro de la calificación de productos sanitarios, considerándose productos o servicios digitales, que estarían protegidos únicamente por la legislación interna de protección de consumidores y usuarios⁹⁸.

Pero, además, debe tenerse en cuenta la capacidad de algunos de estos dispositivos para aprender por sí mismos, derivada de la programación con sistemas de inteligencia artificial, supuesto que no está contemplado en el RPS y para el que debemos acudir al art. 3.1 del RLIA que define un sistema de inteligencia artificial como «un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales».

⁹⁶ Cfr. RPS, considerando 19. También el anexo VIII, en su apartado 3.3. cuando afirma que «los programas informáticos que sirvan para manejar un producto o tengan influencia en su utilización se incluirán en la misma clase que el producto. Si el programa informático es independiente de cualquier otro producto, será clasificado por sí mismo».

⁹⁷ RPS, considerando 21.

⁹⁸ En el mismo sentido, respecto de las “*apps de salud*”, LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit., p.36.

Como puede verse, la definición es, de nuevo, lo suficientemente amplia para abarcar casi todos los productos y servicios digitales en materia de salud: desde los *chatbots* a los que hacíamos referencia al inicio de este trabajo, hasta el software integrado en los *wearables* a través de los cuales se realiza el seguimiento de funciones básicas para el funcionamiento normal del organismo y que pueden incidir, por tanto, en el diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad.

A este respecto, el considerando 47 del RLIA establece que «Los sistemas de IA pueden tener efectos adversos para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de seguridad. En consonancia con los objetivos de la legislación de armonización de la Unión de facilitar la libre circulación de productos en el mercado interior y velar por que solo lleguen al mercado aquellos productos que sean seguros y conformes, es importante prevenir y reducir debidamente los riesgos de seguridad que pueda generar un producto en su conjunto debido a sus componentes digitales, entre los que pueden figurar los sistemas de IA», refiriéndose expresamente a los sistemas de IA utilizados en el sector sanitario, donde los riesgos para la vida y la salud son especialmente elevados, para el diagnóstico y apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, imponiendo que sean «fiables y precisos».

A partir de aquí, la normativa europea parte del «riesgo» como base fundamental de una regulación dirigida a la prevención y no a la reparación del daño.

Así, el RPS clasifica, en su Anexo VIII, los productos sanitarios en cuatro categorías (I, IIa, IIb y III) en función de la finalidad prevista de los productos y de su mayor o menor riesgo para el usuario⁹⁹. A estos efectos, los productos a los que nos referimos en el presente trabajo quedarían encuadrados originariamente en la categoría I al tratarse de productos «no invasivos» y «productos activos para diagnóstico y vigilancia», entendiéndose por tales «cualquier producto activo, utilizado solo o en combinación con otros productos, destinado a proporcionar información para la detección, el diagnóstico, la observación o el tratamiento de estados fisiológicos, de estados de salud, de enfermedades o de malformaciones congénitas»¹⁰⁰, si bien deben tenerse en cuenta las siguientes excepciones¹⁰¹:

⁹⁹ En líneas generales, y sin perjuicio de las especificidades que el propio anexo establece, los productos no invasivos se incluyen en la clase I, mientras que los productos invasivos se incluyen en las clases IIa, IIb y III en función de su finalidad, uso prolongado o pasajero, y mayor riesgo.

¹⁰⁰ Anexo VIII, apartado 2.5 RPS.

¹⁰¹ Anexo VIII, apartado 6.3, regla 11 RPS.

- Programas informáticos destinados a proporcionar información que se utilice para observar procesos fisiológicos o tomar decisiones con fines terapéuticos o de diagnóstico (clase IIa).
- Programas informáticos dedicados a observar parámetros fisiológicos vitales, cuando la índole de las variaciones de dichos parámetros sea tal que pudiera dar lugar a un peligro inmediato para el paciente (clase IIb).
- Programas informáticos cuya toma de decisiones pueda suponer la muerte o un deterioro irreversible del estado de salud de una persona (clase III).

Por su parte, el RLIA realiza una clasificación de las prácticas o sistemas de IA en tres categorías distintas, dependiendo de la intensidad del riesgo¹⁰²:

a) *Prácticas de inteligencia artificial prohibidas (Capítulo II)*: Se consideran especialmente peligrosas aquellas prácticas de inteligencia artificial que se utilicen para «persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente» y, por ello, se prohíbe «la introducción en el mercado, la puesta en servicio o la utilización de determinados sistemas de IA con el objetivo o al efecto de alterar de manera sustancial el comportamiento humano, con la consiguiente probabilidad de que se produzcan perjuicios considerables, en particular, perjuicios con efectos adversos suficientemente importantes en la salud física o mental o en los intereses financieros». También se prohíben los sistemas de IA que exploten «las vulnerabilidades de una persona o un grupo específico de personas derivadas de su edad, su discapacidad en el sentido de lo dispuesto en la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo o de una situación social o económica concreta que probablemente aumente su vulnerabilidad a la explotación, como vivir en condiciones de pobreza extrema o pertenecer a minorías étnicas o religiosas»¹⁰³. Por último, dentro de este grupo se refiere también el RLIA a los «sistemas de categorización biométrica basados en datos biométricos de las personas, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas

¹⁰² Como se ha dicho, en este sentido, las actividades prohibidas no suponen en todos los casos actividades directas y necesariamente lesivas, sino generadoras de un riesgo inaceptable. Por su parte, los supuestos no sometidos a la regulación de alto riesgo, se sostienen sobre una valoración de su riesgo como menor, asumible de forma general. MACANÁS, G.: “Mutualización de los riesgos generados por los sistemas de IA”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por el autor), p. 3.

¹⁰³ RLIA, Considerando (29).

o filosóficas, la raza, la vida sexual o la orientación sexual de las personas»¹⁰⁴, a los «sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas»¹⁰⁵ y al uso de sistemas de IA para la identificación biométrica remota «en tiempo real»¹⁰⁶.

b) *Sistemas de IA de alto riesgo (Capítulo III)*. Un sistema de IA se considera de alto riesgo en función de su finalidad prevista, conforme a la legislación vigente relativa a la seguridad de los productos. Por lo tanto, la clasificación de un sistema de IA como de alto riesgo no depende únicamente de la función que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se use dicho sistema, definiéndose, en el art. 6 las dos categorías principales de sistemas de IA de alto riesgo:

1. Los sistemas de IA diseñados para utilizarse como componentes de seguridad de productos que entren en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos; y que el producto del que el sistema de IA sea componente de seguridad esté sujeto a una evaluación de la conformidad ex ante realizada por terceros. No obstante, un sistema de IA no se considerará de alto riesgo si no plantea un *riesgo importante* de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, en particular *al no influir sustancialmente en el resultado de la toma de decisiones*¹⁰⁷.
2. Otros sistemas de IA independientes con implicaciones relacionadas principalmente con los derechos fundamentales, los cuales se indican explícitamente en el anexo III¹⁰⁸.

¹⁰⁴ RLIA Considerando (30).

¹⁰⁵ RLIA Considerando (31).

¹⁰⁶ RLIA, Considerandos (32 a 39).

¹⁰⁷ El art. 6.3 RLIA somete esta excepción al cumplimiento de una o varias de las condiciones siguientes: a) que el sistema de IA tenga por objeto llevar a cabo una tarea de procedimiento limitada; b) que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada; c) que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; d) que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III.

¹⁰⁸ La lista de sistemas de IA de alto riesgo que figura en el anexo III contiene un número limitado de sistemas de IA cuyos riesgos ya se han materializado o es probable que lo hagan próximamente. La Comisión podría ampliar la lista de sistemas de IA de alto riesgo utilizados en determinados ámbitos predefinidos mediante la aplicación de un conjunto de criterios y una metodología de evaluación del riesgo, a fin de garantizar que el Reglamento pueda adaptarse a los nuevos usos y aplicaciones de la IA.

c) *Modelos de IA de Uso General (Capítulos IV y V)*: Todos los sistemas de IA que no se encuentren entre las prácticas prohibidas o los sistemas de alto riesgo, entran dentro de las reglas de clasificación de los modelos de IA de uso general, dentro de los cuales se crea una subcategoría específica para los «modelos de IA de uso general con riesgo sistémico» (art. 51) que son aquellos que «tienen capacidades de gran impacto» evaluadas, bien a partir de herramientas y metodologías técnicas adecuadas, como podrían ser indicadores y parámetros de referencia, bien a partir de una decisión de la Comisión¹⁰⁹ adoptada de oficio, o a raíz de una alerta cualificada del grupo de expertos científicos.

Para los proveedores de modelos de IA de uso general el RLIA establece obligaciones de elaboración y mantenimiento de la documentación técnica del modelo y de la información relativa al mismo (art. 53), así como la obligación de designar, mediante mandato escrito, a un representante autorizado que esté establecido en la Unión, antes de introducir en el mercado un modelo de IA de uso general (art. 54).

Además de estas obligaciones, los proveedores de modelos de IA de uso general con riesgo sistémico deben evaluar los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, así como evaluar y reducir los posibles riesgos sistémicos que puedan derivarse de la introducción en el mercado de la Unión de sus modelos de IA, vigilando, documentando y comunicando la información pertinente sobre incidentes graves y posibles medidas correctoras, y velando por el establecimiento de un nivel adecuado de protección de la ciberseguridad para el modelo de IA (art. 55).

En cuanto a los sistemas de IA, asociados a aplicaciones, chatbots, werables o dispositivos de *m-health*, en particular cuando funcionan como componentes

¹⁰⁹ Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos de «gran impacto» el Anexo XIII del RLIA establece que la Comisión tendrá en cuenta los siguientes criterios: a) el número de parámetros del modelo; b) la calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas; c) la cantidad de cálculo utilizada para entrenar el modelo, medida en FLOP o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo; d) las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas); e) los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su grado de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso; f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10.000 usuarios profesionales registrados establecidos en la Unión; g) el número de usuarios finales registrados.

de seguridad de productos, o como productos en sí mismos, tratándose de sistemas de diagnóstico, y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, el RLIA exige que sean «seguros» «conformes», «fiables» y «precisos», previniendo y reduciendo debidamente los riesgos de seguridad que pueda generar el producto en su conjunto, debido a sus componentes digitales, entre los que pueden figurar los sistemas de IA.¹¹⁰ En consonancia con ello, se califican como «de alto riesgo» los sistemas de IA que son componentes de seguridad de producto, o que son productos en sí mismos, cuando el producto en cuestión es sometido a un procedimiento de evaluación de la conformidad con un organismo independiente de evaluación de la conformidad, de acuerdo con la legislación de armonización de la Unión, tal y como ocurre, entre otros, con los «productos sanitarios»¹¹¹.

Además, que un sistema de IA se considere de alto riesgo en virtud del RLIA, no significa necesariamente que el producto del que sea componente de seguridad, o el sistema de IA en sí mismo como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto¹¹², tal y como ocurre expresamente con los productos sanitarios regulados por el RPS, que prevé que un organismo independiente realice la evaluación de la conformidad de los productos calificados por el propio Reglamento como de riesgo medio y alto.

Por último, en relación a los sistemas de IA independientes, es decir, aquellos que no sean componentes de seguridad de productos o no puedan ser considerados productos en sí mismos, también procede calificarlos como «de alto riesgo» cuando, a la luz de su finalidad prevista, presenten un alto riesgo de ser perjudiciales para la *salud* y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca¹¹³.

En conclusión, creemos que la finalidad médica de muchos de los productos o sistemas informáticos a los que nos referimos en el presente trabajo, permite su consideración como «productos sanitarios» y su clasificación como tales en función del riesgo generado, que en el caso de los sistemas de IA incorporados como componentes de seguridad o considerados productos en sí mismos, sería el nivel de «riesgo alto». No obstante, la ausencia de referencia expresa a los mismos en el RPS deja en manos del fabricante y de los propios Estados su calificación como «productos sanitarios» o como pro-

¹¹⁰ Cfr. Considerando 47 del RLIA.

¹¹¹ Cfr. Considerando 50 del RLIA.

¹¹² Cfr. Considerando 51 del RLIA.

¹¹³ Cfr. Considerando 52 del RLIA.

ductos de consumo para finalidades de bienestar, deportivas, etc., que, sin duda, incidirán en una mayor distribución y comercialización. En este sentido, el considerando 8 del RPS establece que «debe ser responsabilidad de los Estados miembros decidir en cada caso si un producto entra o no en el ámbito de aplicación del presente Reglamento. Para garantizar unas decisiones de cualificación coherentes al respecto en todos los Estados miembros, en especial en lo que se refiere a los *casos frontera*, la Comisión debe estar autorizada para decidir en cada caso, por propia iniciativa o en respuesta a una solicitud debidamente justificada de un Estado miembro, y previa consulta al Grupo de Coordinación de Productos Sanitarios (MDCG), si un producto específico, una categoría o un grupo de productos entran o no en el ámbito de aplicación del presente Reglamento», sin que, hasta el momento, se haya producido pronunciamiento alguno, respecto de los productos tratados en este estudio.

3.2. SUJETOS RESPONSABLES

A la hora de determinar el sujeto responsable, las diferentes normas realizan una delimitación plural de los mismos.

Así, por un lado, el RPS delimita las obligaciones generales de los «fabricantes»¹¹⁴; «importadores»¹¹⁵; y «distribuidores»¹¹⁶, especificando los casos en que las obligaciones de los fabricantes se extienden a los importadores, distribuidores u otras personas (art. 16). Por otro lado, el RLIA se refiere en su art. 3 como posibles «operadores» al «proveedor»¹¹⁷, «responsable del despliegue»¹¹⁸, «re-

¹¹⁴ Toda persona física o jurídica que fabrica, renueva totalmente o manda diseñar, fabricar o renovar totalmente un producto, y lo comercializa con su nombre o marca comercial (art. 2.30 RPS), pudiendo actuar por sí mismo o por representante autorizado en base a mandato escrito (art. 2.32 RPS).

¹¹⁵ Toda persona física o jurídica establecida en la Unión que introduce un producto procedente de un tercer país en el mercado de la Unión (art. 2.33 RPS).

¹¹⁶ Toda persona física o jurídica de la cadena de suministro, distinta del fabricante o el importador, que comercializa un producto, hasta el momento de ponerlo en servicio (art. 2.34 RPS).

¹¹⁷ «Una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos, que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente».

¹¹⁸ «Una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional». En el supuesto que estamos tratando, el médico que hace uso del sistema de IA con finalidad profesional sería considerado «responsable del despliegue».

presentante autorizado»¹¹⁹, «importador»¹²⁰ y «distribuidor»¹²¹. Por último, la DRPD se refiere, en su art. 4, como «operadores económicos» al «fabricante»¹²², «representante autorizado»¹²³, «importador»¹²⁴, «distribuidor»¹²⁵, añadiendo al «prestador de servicios de tramitación de pedidos a distancia»¹²⁶.

En todos los casos, la responsabilidad principal corresponde al «fabricante» o «proveedor». En este sentido, a pesar de no coincidir exactamente ambas definiciones, creemos que la introducción en el mercado o la puesta en servicio con su propio nombre o marca comercial, que caracteriza al «proveedor» en el ámbito del RLIA hace que su concepto sea coincidente con el de «fabricante» en la mayoría de ocasiones, pudiendo actuar por sí mismos o por medio de representante autorizado mediante mandato. En cuanto a los conceptos de «importador» y «distribuidor» no plantean contradicciones entre sí.

Si el producto se calificase como sanitario, en el sentido que hemos expuesto, la primera obligación que corresponde al fabricante es la de superar un procedimiento de evaluación de dicho producto, antes de obtener el marcado CE y de que se proceda a su comercialización¹²⁷, clasificándose los productos sanitarios en cuatro clases (I, IIa, IIb y III), en función de la finalidad prevista y de los riesgos inherentes, haciendo más estricto el procedimiento de evaluación de la conformidad conforme el proyecto esté clasificado en una clase superior y, por tanto, implique mayor riesgo para el usuario¹²⁸.

¹¹⁹ Toda persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento, en representación de dicho proveedor».

¹²⁰ «Una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida en un tercer país».

¹²¹ «Una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión».

¹²² «Toda persona física o jurídica que: a) desarrolla, fabrica o produce un producto; b) tiene un producto diseñado o fabricado, o que, al poner su nombre, marca u otros elementos distintivos en dicho producto, se presenta como su fabricante; o c) desarrolla fabrica o produce un producto para su propio uso».

¹²³ «Toda persona física o jurídica establecida en la Unión que ha recibido un mandato escrito de un fabricante para actuar en su nombre en tareas específicas».

¹²⁴ «Toda persona física o jurídica que introduzca en el mercado de la Unión un producto de un tercer país».

¹²⁵ «Toda persona física o jurídica de la cadena de suministro, distinta del fabricante o el importador, que comercialice un producto».

¹²⁶ «Toda persona física o jurídica que ofrezca, en el transcurso de su actividad comercial, al menos dos de los siguientes servicios: almacenar, embalar, dirigir y despachar un producto, sin tener la propiedad del mismo; con la excepción de los servicios postales, de paquetería y cualquier otro servicio postal o de transporte de mercancías».

¹²⁷ Art. 20 RPS.

¹²⁸ Cfr. art. 51(1) y Anexo VIII RPS.

Como expusimos anteriormente, los productos digitales a los que hacemos referencia en el presente trabajo, estarían clasificados originariamente en la clase I, al considerarse productos activos no invasivos, «destinados a proporcionar información para la detección, el diagnóstico, la observación o el tratamiento de estados fisiológicos, de estados de salud, de enfermedades o de malformaciones congénitas»¹²⁹, si bien, en la actualidad, la práctica totalidad de programas informáticos encuadrados en el ámbito de la *m-health*, también proporcionan información que puede utilizarse para observar procesos fisiológicos o tomar decisiones con fines terapéuticos o de diagnóstico, por lo que, en su mayoría, estarían clasificados en la clase IIa, salvo que estén dedicados a observar parámetros fisiológicos vitales, cuando la índole de las variaciones de dichos parámetros sea tal que pudiera dar lugar a un peligro inmediato para el paciente (clase IIb); o, finalmente, cuando la toma de decisiones pueda suponer la muerte o un deterioro irreversible del estado de salud de una persona, en cuyo caso estarían clasificados en la clase III¹³⁰.

Cuando la clasificación del producto corresponda a la clase I, el procedimiento de evaluación de la conformidad puede llevarse a cabo bajo la exclusiva responsabilidad del fabricante, sin intervención de un organismo notificado. En los casos restantes, el procedimiento deberá realizarse bajo la supervisión de un organismo notificado.

En segundo lugar, los fabricantes deben elaborar la documentación técnica de acuerdo con lo establecido en el Anexo II RPS, incluyendo una descripción general de los elementos funcionales clave, un análisis del riesgo-beneficio y una justificación, validación y verificación de las soluciones adoptadas para cumplir los requisitos generales de seguridad y funcionamiento.

Además, deben realizar un plan de vigilancia post-comercialización, en el que se incluya, entre otras cosas, la recogida de información de los usuarios del producto sobre incidentes graves y no graves, reclamaciones y otras reacciones.

Por último, corresponde al fabricante proporcionar información a los usuarios acerca del uso de estos dispositivos. En este sentido, el art. 7 RPS prohíbe el uso de textos, denominaciones, marcas comerciales, fotografías e imágenes u otros signos que puedan inducir a error al usuario en cuanto a la finalidad prevista, la seguridad y el funcionamiento del producto por alguno de los siguientes medios:

- a) Atribuir al producto funciones y propiedades que no tiene.

¹²⁹ Cfr. Anexo VIII, apartado 2.5 RPS.

¹³⁰ Anexo VIII, apartado 6.3, regla 11 RPS.

- b) Crear una falsa impresión sobre tratamiento o diagnóstico, funciones o propiedades que el producto no posee.
- c) No informar al usuario o al paciente sobre los posibles riesgos que conlleva la utilización del producto conforme a su finalidad prevista.
- d) Dar a entender usos del producto diferentes de los indicados como parte de la finalidad prevista para la que se realizó la evaluación de la conformidad.

Además, el Anexo I n° 23(1) RPS exige a los fabricantes «proporcionar información pertinente sobre la seguridad y el funcionamiento para el usuario o cualquiera otra persona, según proceda», adaptada a «los conocimientos técnicos, la experiencia, la educación o la formación de los usuarios previstos». Esta información debe destacar los beneficios clínicos que cabe esperar y las características de funcionamiento del producto¹³¹.

Como se ha puesto de manifiesto¹³², debe extremarse el cumplimiento del deber de información al usuario de unas aplicaciones de funcionamiento muy sencillo e intuitivo, que atraen fácilmente la atención de pacientes y personas en situación de vulnerabilidad, pero que no han sido concebidas como sustitutivo de la actividad médica. El propio Parlamento Europeo ha alertado, en este sentido, del incremento del autodiagnóstico, incidiendo en la necesidad de que los usuarios y también los sanitarios estén formados e informados en las nuevas tecnologías, para que su uso no provoque un aumento del error humano y, en consecuencia, una reducción de la esperanza y calidad de vida de las personas.

En cuanto a los sistemas de IA de alto riesgo, incorporados a productos que puedan ser calificados como sanitarios, el RLIA complementa lo establecido en el RPS, ya que los requisitos esenciales de los sistemas de IA de alto riesgo deben evaluarse como parte del procedimiento de evaluación de la conformidad del RPS, siendo responsable el fabricante del producto de que el sistema de IA de que se trate cumpla lo dispuesto en el RLIA y, por lo que al sistema de IA se refiere, teniendo el fabricante las mismas obligaciones que el RLIA impone al proveedor¹³³.

Las obligaciones de los proveedores de sistemas de IA de alto riesgo vienen establecidas de forma genérica en el art. 16 del RLIA, y desarrolladas en

¹³¹ Cfr. Anexo I n° 23 (4) RPS.

¹³² LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit, p. 28.

¹³³ Sobre la posible confluencia de disposiciones referidas a los sujetos responsables respecto de sistemas de IA vid. ORTIZ FERNÁNDEZ, M.: “El derecho de daños ante la inteligencia artificial: la intervención de la Unión Europea”, *Actualidad Jurídica Iberoamericana*, n° 18, febrero 2023, pp. 1313-1315.

los artículos posteriores, en el sentido de: velar porque el sistema de IA cumpla los requisitos de gestión de riesgos, datos y gobernanza de datos, documentación técnica, conservación de registros, accesibilidad, transparencia y comunicación de información a los responsables del despliegue, vigilancia humana, precisión solidez y ciberseguridad, establecidos en la sección segunda (arts. 8 a 15) del RLIA; identificación del propio proveedor en el sistema o en el embalaje del sistema; contar con un sistema de gestión de calidad; conservación de la documentación y de los archivos de registros; sometimiento al procedimiento pertinente de evaluación de la conformidad; marcado CE del sistema o de su embalaje; adopción de medidas correctoras cuando el sistema no sea conforme, para retirarlo del mercado, desactivarlo o recuperarlo e información inmediata a los distribuidores, importadores y responsables del despliegue.

El criterio esencial sobre el que se basa la exigencia de responsabilidad en estos casos es el *control* que el fabricante o proveedor ejerce sobre el riesgo asociado al funcionamiento del sistema de IA¹³⁴, por lo que el organismo notificado, encargado de realizar la evaluación de la conformidad, debe revisar también los requisitos específicos establecidos en el RLIA que acabamos de mencionar.

La obligación de transparencia y comunicación de información establecida en el art. 13 del RLIA se convierte, a estos efectos, en fundamental al imponer la garantía de un tipo y un nivel de transparencia adecuados para que el usuario y el proveedor cumplan con las obligaciones oportunas previstas en la sección 3, obligando, además, a que los sistemas de IA de alto riesgo vayan acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, incluyendo información *concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios*, que haga referencia a:

- a) La identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado.
- b) Las características, capacidades y limitaciones del funcionamiento del sistema¹³⁵.

¹³⁴ Control entendido como *influencia* (posibilidad de influir) en el funcionamiento del sistema. LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit. p. 50.

¹³⁵ En particular se refiere entre ellas el art. 13 a: su finalidad prevista, el nivel de precisión (incluidos los parámetros para evaluarla), solidez y ciberseguridad con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y qué puede esperarse, así como cualquier circunstancia conocida y previsible que pueda afectar al nivel de precisión, solidez y ciberseguridad esperado; cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lu-

- c) Los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso.
- d) Las medidas de vigilancia humana, a que hace referencia el art. 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue.
- e) Los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias (incluida su frecuencia) para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a las actualizaciones del software.
- f) Cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el art. 12.

No obstante, esta obligación de transparencia y comunicación de información del proveedor se establece respecto de los «responsables del despliegue», es decir, respecto de los que podrían ser definidos como «usuarios profesionales» del sistema de IA de alto riesgo, pero no respecto del destinatario o usuario final.

Precisamente, en relación a la información proporcionada al usuario no profesional o destinatario final del sistema, creemos especialmente importante que se incluya en sistema de IA de alto riesgo, la información relativa a la funcionalidad del producto y de los contenidos digitales, de acuerdo con lo que el usuario pueda razonablemente esperar. De esta forma, algunas de las características, capacidades y limitaciones del funcionamiento del sistema incluidas en el art. 13 b) del RLIA como obligación de información «para que los responsables del despliegue interpreten y usen correctamente la información de salida» deberían ampliarse al destinatario final del sistema, en particular:

gar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere el artículo 9, apartado 2; en su caso, las capacidades y características técnicas del sistema de IA de alto riesgo para proporcionar información pertinente para explicar su información de salida; cuando proceda, su funcionamiento con respecto a personas o grupos de personas específicos en relación con los que esté previsto utilizar el sistema; cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA; en su caso, información que permita a los responsables del despliegue interpretar la información de salida del sistema de IA de alto riesgo y utilizarla adecuadamente.

- La finalidad prevista del sistema.
- Cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales. En nuestra opinión, el criterio de la *razonabilidad previsible* debe ser objetivamente determinable teniendo en cuenta la naturaleza y la finalidad del bien, contenido o servicio contratado, las circunstancias del caso y los usos y prácticas de las partes implicadas.
- Cuando proceda, su funcionamiento con respecto a personas o grupos de personas específicos en relación con los que esté previsto utilizar el sistema, especialmente en aquellos sistemas de IA dirigidos a colectivos especialmente vulnerables como los ancianos o las personas dependientes.

Esta obligación de información se convierte en esencial si tenemos en cuenta la incidencia que la conducta de dicho usuario puede tener en la delimitación de la responsabilidad. A esta cuestión responde el considerando 29 de la PDRIA, cuando, «a fin de lograr un equilibrio entre los intereses de los perjudicados y los de los usuarios no profesionales», tiene en cuenta si dichos usuarios no profesionales pueden aumentar, mediante su comportamiento, el riesgo de que un sistema de IA cause daños. Desde este punto de vista, cuando el usuario no profesional se limita a poner en funcionamiento el producto, de acuerdo con su finalidad, y el proveedor ha cumplido todas sus obligaciones, considerándose que dicho sistema es suficientemente seguro para ser comercializado con vistas a un uso determinado por usuarios no profesionales, no podría aplicarse la presunción de responsabilidad respecto del usuario no profesional. En cambio, si el usuario no profesional ha interferido sustancialmente en las condiciones de funcionamiento de un sistema de IA, o tenía la obligación y estaba en condiciones de determinar las condiciones de funcionamiento y no lo hizo, podría aplicarse respecto del mismo la presunción de responsabilidad, como ocurriría, por ejemplo, cuando el usuario no profesional no respeta las instrucciones de uso u otras obligaciones de diligencia aplicables a la hora de elegir el ámbito de operación o de fijar las condiciones de funcionamiento del sistema de IA.

En nuestra opinión, este criterio resulta perfectamente aplicable para moderar o excluir la responsabilidad cuando es el propio usuario del producto el que interfiere con su conducta en el funcionamiento del mismo, de ahí que sea extremadamente importante la obligación de información a cargo del fabricante.

En cuanto a la posibilidad de extender la responsabilidad a otros sujetos, aplicando un criterio de solidaridad, el art. 16 del RPS permite que la responsabilidad del fabricante/productor pueda aplicarse a los importadores, distribuidores u otras personas cuando concurra alguna de las siguientes circunstancias:

- Comercializar un producto con su propio nombre, nombre comercial registrado o marca registrada, salvo que llegue a un acuerdo con el fabricante para que este se identifique como tal en la etiqueta y sea responsable de cumplir las obligaciones establecidas en el Reglamento.
- Cambiar la finalidad prevista de un producto ya introducido en el mercado o puesto en servicio.
- Modificar un producto ya introducido en el mercado o puesto en servicio, de modo que pueda verse afectado el cumplimiento de los requisitos aplicables.
- Suministrar el producto a sabiendas de la existencia del defecto.

Además, en el ámbito de la responsabilidad por productos defectuosos, a tenor del art. 8.1 DRPD el «importador» y el «representante autorizado del fabricante» asumirán la responsabilidad del fabricante cuando este último esté establecido fuera de la Unión, y sin perjuicio de la responsabilidad del propio fabricante; en cambio, si el importador o el representante autorizado del fabricante también estuvieran establecidos fuera de la Unión la responsabilidad recae en el prestador de servicios de tramitación de pedidos a distancia. Por su parte, la responsabilidad del «distribuidor» parte del supuesto de que el fabricante o el resto de operadores económicos mencionados anteriormente no puedan identificarse o que esté establecido fuera de la Unión, siempre y cuando el demandante solicite al distribuidor dicha identificación y éste no la realice en el plazo de un mes a partir de la recepción de la solicitud (art. 8.3 DRPD).

3.3. CRITERIOS DE IMPUTACIÓN

El criterio de imputación, objetivo o subjetivo, a la hora de establecer la responsabilidad civil por los daños derivados del uso de estos productos o servicios digitales es la cuestión más controvertida que plantea este tema. De hecho, desde la perspectiva del daño indemnizable la digitalización o el uso de la inteligencia artificial no comporta relevancia alguna en un sistema jurídico

como el español, neutro tecnológicamente, y en el cual no rige un principio de tipicidad de los daños indemnizables¹³⁶.

No es, por tanto, la delimitación de los daños indemnizables, su cuantificación y su reparación¹³⁷, lo que plantea interrogantes, sino el criterio de imputación objetiva o subjetiva de los daños en supuestos en los que interviene una tecnología avanzada y conectada, en muchas ocasiones, con modelos de inteligencia artificial. Y, en este sentido, la calificación que reciba el «producto» o sistema de IA incidirá en la delimitación de la normativa aplicable y, en consecuencia, en el sometimiento a un régimen de responsabilidad objetivo o subjetivo.

La clave para establecer el fundamento de la responsabilidad estará en la consideración o no del producto como «sanitario» y en la calificación de sistema de riesgo alto o «de uso general», del sistema de inteligencia artificial incorporado al mismo.

3.3.1. Responsabilidad objetiva

Como hemos visto anteriormente, el RPS utiliza el nivel de riesgo del «producto sanitario» como criterio de imputación a la hora de ampliar la responsabilidad del fabricante, estableciendo un sistema de responsabilidad objetiva para los productos sanitarios, conforme con el que se establece en la responsabilidad derivada de productos defectuosos, exigiendo al fabricante que tome medidas para garantizar una cobertura financiera suficiente con respecto a su posible responsabilidad, y estableciendo que dichas medidas deben ser proporcionadas a la clase de riesgo, el tipo de producto y el tamaño de la empresa¹³⁸.

Además, la regla que se refiere a los programas informáticos utiliza un criterio de mera «posibilidad», al referirse a «un impacto que *pueda causar* un daño», distinto del criterio de la probabilidad causal, con lo cual podría concluirse que «cualquier *posible* consecuencia (grave) para la salud humana puede dar lugar a un aumento de la clase de riesgo»¹³⁹, lo que conducirá de facto a un sistema de responsabilidad objetivo. Este fundamento ha sido criticado

¹³⁶ RUBÍ PUIG, A.: “Inteligencia artificial y daños indemnizables”, Ponencia presentada a las XII Jornadas de la APDC, Granada, octubre-2023 (versión pdf cedida por el autor), p. 2.

¹³⁷ Se pone como ejemplo, en este sentido, que la indemnización de una pérdida de oportunidad ocasionada por un diagnóstico médico erróneo no habría de variar en función de si fue un médico quien diagnosticó a la víctima o, en su caso, un algoritmo para la toma de decisiones médicas. RUBÍ PUIG, A.: Op. loc. cit.

¹³⁸ RPS, considerando 31.

¹³⁹ LUQUIN BERGARECHE, R.: “Responsabilidad contractual...”, cit, p. 39.

en la doctrina sobre la base de que puede «limitar la innovación en el sector sanitario de la UE al entender incluidas dentro de la relación de causalidad todas las posibles causas del daño, aun las más remotas»¹⁴⁰.

En realidad, la introducción de un criterio de causalidad probabilística no sólo afecta a la relación causal entre la conducta y el daño, sino al propio concepto de daño y a la imputación del mismo.

En cuanto al concepto de daño, por cuanto que este ya no se entiende como el desvalor cierto producido por la conducta del agente sino como el incremento probabilístico de que se produzca un daño cierto por efecto del desarrollo de una determinada actividad. Así pues, en base a este criterio no se debe determinar si el daño se produjo o no de manera cierta, sino si la actividad incrementó las posibilidades de que el daño se produzca¹⁴¹, lo cual no parece descabellado.

Respecto a la imputación, por cuanto que la probabilidad de la materialización de un daño puede configurarse como un criterio relevante a la hora de imputar la responsabilidad que deriva del incumplimiento de un deber de diligencia, ya que, cuanto menor sea el grado de cumplimiento de los deberes específicos puestos a cargo de los sujetos responsables, mayor será el nivel de probabilidad de que el riesgo se materialice.

En el RLIA también se utiliza la clasificación en función del riesgo como criterio de imputación de las obligaciones del proveedor de sistemas de IA de alto riesgo. No obstante, las categorías de riesgos incluidas en el RLIA difieren de las del RPS, ya que mientras el RLIA incluye a todos los productos sanitarios en la categoría de «alto riesgo», en el RPS, dichos productos pueden englobarse tanto en la clase I (riesgo bajo), como en las clases IIa y IIb (riesgo medio), o en la clase III (riesgo alto). En nuestra opinión, esta aparente contradicción está resuelta en el propio RLIA en cuanto establece que el hecho de que un sistema de IA se considere de alto riesgo, no significa necesariamente que el producto del que sea componente de seguridad, o el sistema de IA en sí mismo como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto¹⁴².

No obstante, a la hora de determinar el nivel de riesgo, el RLIA se aleja del criterio de posibilidad establecido en el RPS al referirse a la «identificación y análisis de los riesgos conocidos y previsibles que el sistema de IA de

¹⁴⁰ *Op. loc. cit.* La autora propone como solución sustituir este parámetro por el de «criterios razonables de probabilidad».

¹⁴¹ BULLARD GONZÁLEZ, A.: "Causalidad probabilística: El problema de los costos administrativos en el diseño de un sistema de responsabilidad civil extracontractual", *Ius et Veritas*, 1991, 2(3), p. 7. Recuperado a partir de <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15312>

¹⁴² Cfr. Considerando 51 RLIA.

alto riesgo pueda conllevar para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista» (art. 9.2.a.), así como a la «estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un *uso indebido razonablemente previsible*» (art. 9.2.b.).

De esta forma, frente al criterio de la *posibilidad* establecido en el RPS, el RLIA utiliza el criterio de la *previsibilidad razonable*, para configurar el nivel de exigibilidad aplicable a los operadores económicos. Como acertadamente se ha dicho en la doctrina¹⁴³, la previsibilidad se ha presentado como uno de los obstáculos más importantes a la hora de aplicar un régimen de responsabilidad por culpa en la IA, utilizándose, bajo la fórmula de la causalidad adecuada o adecuación en el marco de la imputación objetiva, para limitar la responsabilidad a aquellos daños que el autor de la acción u omisión dañosa pudo haber razonablemente previsto, si bien, el problema será que ninguno de los potenciales sujetos responsables va a ser capaz de prever la decisión que va a adoptar el sistema.

Ha desaparecido, sin embargo, del texto definitivo del RLIA la referencia al «estado actual de la técnica generalmente reconocido, que, entre otras fuentes, está reflejado en las normas armonizadas o las especificaciones comunes pertinentes» que se realizaba en el art. 9.3, antes de la Resolución del Parlamento Europeo de 13 de marzo de 2024, y que suponía una clara referencia a un régimen culpabilístico basado en la *lex artis*, sustituyéndose dicha referencia por la de que «los riesgos a que se refiere el presente artículo son únicamente aquellos que pueden reducirse o eliminarse *razonablemente* mediante el desarrollo o el diseño del sistema de IA de alto riesgo o el suministro de información técnica adecuada».

También en el ámbito de la responsabilidad por productos defectuosos se utiliza un criterio de imputación objetivo, al considerarse el único medio de abordar adecuadamente el problema de un reparto justo del riesgo inherente a la producción técnica moderna¹⁴⁴. Dicho criterio de imputación objetivo está basado en el carácter defectuoso del producto, la prueba del daño y el nexo de causalidad entre ambos, sin que la actuación diligente de los sujetos llamados a responder pueda ser tomada en consideración a la hora de moderar o exonerar la responsabilidad.

¹⁴³ PEÑA LÓPEZ, F.: «Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la inteligencia artificial (provisional 03/10/23)», Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por el autor), p. 12.

¹⁴⁴ Cfr. Considerando 2 DRPD.

En cuanto al concepto de «defectuosidad», el art. 7 considera un producto como defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o del Derecho nacional. No obstante, en relación a este criterio, la propia Directiva aclara que la evaluación del carácter defectuoso de un producto debe incluir un análisis objetivo de la seguridad que «el público en general» tiene derecho a esperar y no referirse a la seguridad que una persona concreta tiene derecho a esperar¹⁴⁵. Este análisis objetivo de la seguridad debe evaluarse, teniendo en cuenta, entre otras cosas, la finalidad prevista del producto, su uso «razonablemente previsto», la presentación, las características objetivas y las propiedades del producto de que se trate, incluido su ciclo de vida previsto, así como las necesidades específicas del grupo de usuarios al que se destina el producto.

En relación a los productos sanitarios de «soporte vital», dado el riesgo de daños especialmente elevado que conllevan para las personas, generan a la vez unas expectativas de seguridad especialmente elevadas. Para tener en cuenta estas expectativas, la DRPD¹⁴⁶ establece una «presunción cualificada de defectuosidad» en el sentido de poder considerar defectuoso un producto sin demostrar su defectuosidad real, cuando pertenezca a la misma serie de producción que un producto cuyo carácter defectuoso ya ha sido probado. Esta consideración podría aplicarse, por ejemplo, respecto de los *wereables* que comunican caídas de los usuarios para preservar su vida o su integridad.

A pesar del establecimiento de un régimen de responsabilidad objetivo, la DRPD es consciente de la situación de desventaja significativa en la que se encuentran las personas perjudicadas frente a los fabricantes en cuanto al acceso y la comprensión de la información sobre cómo se ha fabricado un producto y cómo funciona, socavando el reparto equitativo del riesgo, en particular en los casos de complejidad técnica o científica¹⁴⁷.

Para paliar esa asimetría se establecen dos tipos de medidas, de conformidad con el nivel de prueba aplicable con arreglo al Derecho nacional:

En primer lugar, se facilita el acceso de los demandantes a las pruebas que vayan a utilizarse en los procedimientos judiciales, garantizando al mismo tiempo que ese acceso se limite a lo necesario y proporcionado, y que la información confidencial y los secretos comerciales estén protegidos (art. 9 DRPD).

¹⁴⁵ Cfr. Considerando 30 DRPD.

¹⁴⁶ Considerando 30.

¹⁴⁷ Considerando 42.

En segundo lugar, estableciendo presunciones de defectuosidad de un producto, del nexo causal entre el daño y el defecto, o de ambos, con la finalidad de aligerar la carga de la prueba del demandante, cuando el demandado incumpla la obligación de revelar información; cuando se incumplan los requisitos de seguridad obligatorios; en los supuestos de «funcionamiento defectuoso evidente» durante un uso razonablemente previsible; o cuando, a pesar de cumplir el demandante con la obligación de revelar información, resulte excesivamente difícil para el demandante, habida cuenta de la complejidad técnica o científica del caso, demostrar el carácter defectuoso del producto, o el nexo causal con el daño, o ambas cosas (art.10 DRPD). Para este último supuesto, la complejidad técnica o científica debe ser determinada por los órganos jurisdiccionales nacionales, caso por caso, teniendo en cuenta diversos factores¹⁴⁸:

- La naturaleza compleja del producto, como sería el supuesto de «productos sanitarios innovadores».
- La naturaleza compleja de la tecnología utilizada, como es el caso del «aprendizaje automático».
- La naturaleza compleja de la información y los datos que debe analizar el demandante.
- La naturaleza compleja del nexo causal, como podría ser la relación entre el uso de un «producto sanitario» y la aparición o desarrollo de una enfermedad; o una prueba que exigiera al demandante explicar el funcionamiento interno de un sistema de inteligencia artificial.

De igual forma, la valoración de las «dificultades excesivas» para demostrar la «defectuosidad» del producto, el nexo causal con el daño, o ambos, también debe ser realizada por los órganos jurisdiccionales nacionales, caso por caso, sin exigir al demandante la prueba de tales dificultades, aunque sí la «probabilidad» de las mismas y, dando al demandado la posibilidad de impugnar la existencia de dichas dificultades¹⁴⁹.

En relación al tiempo durante el cual cabe hacer efectiva la responsabilidad objetiva derivada de la defectuosidad del producto, la DRPD se refiere a «plazos de prescripción» (art. 16), por un lado, y a «plazo de caducidad» (art. 17), por otro.

En relación al «plazo de prescripción», el art. 16 DRPD se refiere al plazo en el cual debe producirse la incoación de procedimientos para reclamar la indemnización por los daños incluidos en el ámbito de aplicación de la

¹⁴⁸ Cfr. DRPD Considerando 48.

¹⁴⁹ Cfr. DRPD Considerando 48.

Directiva. Dicho plazo de prescripción es de tres años contados a partir del día en que la persona tuvo conocimiento «o debería haber tenido razonablemente conocimiento» de los daños; del carácter defectuoso del producto; y de la identidad del operador económico pertinente que pueda ser considerado responsable de los daños, respetándose, en todo caso, las reglas de Derecho nacional que regulen la suspensión o la interrupción de la prescripción. Del entendimiento del precepto se deduce, claramente, que el *dies a quo* del plazo de prescripción depende de que se conozcan la totalidad de las circunstancias expresadas en el mismo, no comenzando el cómputo mientras una de ellas resulte desconocida.

En cuanto al «plazo de caducidad», el art. 17 lo considera como el plazo durante el cual el perjudicado tiene derecho a una indemnización. En realidad, tal y como está configurado se trata de un auténtico plazo de garantía, en el cual se mantiene efectiva la responsabilidad objetiva derivada de la Directiva. Dicho plazo de garantía se establece, con carácter general, en un periodo de diez años desde la fecha de introducción en el mercado o puesta en servicio del producto defectuoso que causó el daño; o en el caso de productos modificados sustancialmente, desde la fecha de comercialización o puesta en servicio de dicho producto tras su modificación sustancial. Para el supuesto de daños corporales, el plazo de garantía se amplía a veinticinco años.

De esta forma, siempre que el perjudicado incoe el procedimiento dentro de los mencionados plazos de caducidad (sic. garantía), se aplicará el régimen de responsabilidad objetiva y las reglas facilitadoras de la prueba establecidas en la DRPD. Una vez superado el plazo de caducidad (sic. garantía) no puede decirse que desaparezca la responsabilidad de los operadores económicos, pero el perjudicado deberá demandar conforme al régimen general establecido para cada estado miembro. En el caso de los sistemas de IA incorporados a productos o que constituyan productos en sí mismos, dicho régimen general de responsabilidad estará afectado por la PDRIA.

Por último, la DRPD (art. 11) introduce una serie de circunstancias eximentes específicas para el demandado:

Así, un primer grupo de causas afectan a la actividad que el operador económico realiza en el mercado. En este sentido, están exonerados de responsabilidad los fabricantes o importadores que no han introducido el producto en el mercado ni lo han puesto en servicio; y los distribuidores que no han comercializado el producto.

Un segundo grupo de circunstancias afectan a la «defectuosidad del producto», eximiéndose de responsabilidad a los operadores económicos cuando sea «probable que el defecto que causó el daño no existiera en el momento

que el producto fue introducido en el mercado, puesto en servicio o comercializado, o que el defecto se produjo después de ese momento. No obstante, dado que las tecnologías digitales permiten a los fabricantes ejercer control sobre el producto más allá del momento de la introducción en el mercado o la puesta en servicio, los fabricantes deben seguir siendo responsables de las deficiencias que se produzcan después de ese momento como resultado de programas informáticos o servicios conexos que estén bajo el control del fabricante, ya sea en forma de mejoras o actualizaciones o de algoritmos de aprendizaje automático.

También se exonera de responsabilidad a los operadores económicos cuando el defecto del producto se derive del cumplimiento de los requisitos legales.

Además, se establece una exoneración de responsabilidad para los operadores económicos cuando demuestren «que el estado de los conocimientos científicos y técnicos, en el momento en que el producto fue introducido en el mercado, puesto en servicio, o durante el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso». Dicho estado de conocimientos científicos y técnicos será determinado «con referencia al nivel más avanzado de conocimiento objetivo accesible y no al conocimiento efectivo del operador económico en cuestión, durante el período en que el producto estaba bajo el control del fabricante, era tal que no podía descubrirse su carácter defectuoso»¹⁵⁰. Esta cláusula de exoneración es la que más problemas plantea por las siguientes razones:

En primer lugar, por cuanto que la remisión al «estado de los conocimientos científicos y técnicos», supone una delimitación de la responsabilidad del fabricante en base a la *lex artis ad hoc* y a los riesgos del desarrollo, lo que implica la introducción de una causa de exoneración propia del sistema de responsabilidad fundamentado en la culpa. Como acertadamente se ha observado, en este sentido, la invocación del estado de la ciencia y de la técnica para exonerarse de responsabilidad implica, seguramente, la introducción de ciertos perfiles subjetivos en una responsabilidad de tipo objetivo ya que, atender a la posibilidad de descubrir el defecto con base en conocimientos científicos y técnicos no es otra cosa que valorar la diligencia del productor como buen profesional, y esa injerencia de la culpa parece discordante en una responsabilidad objetiva¹⁵¹. Por ello, se ha reclamado la eliminación de esta cláusula de exoneración, al menos respecto de los daños causados por sistemas de in-

¹⁵⁰ DRPD, considerando 52.

¹⁵¹ ASÍ, ATIENZA NAVARRO, M.L.: “La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora), pp. 37-38

teligencia artificial, lo cual supondría una responsabilidad de los operadores económicos basada exclusivamente en un fundamento de tipo objetivo, sin posibilidad de exoneración por el hecho de no haber podido prever o evitar los daños con base al estado de la ciencia o de la técnica¹⁵².

En segundo lugar, en una materia basada en una constante «carrera» por controlar el mercado tecnológico puede ser extraordinariamente difícil establecer ese «nivel más avanzado de conocimiento objetivo accesible» que supere al «conocimiento efectivo del fabricante», ya que el primero, en la mayoría de los casos permanecerá oculto, determinándose al final la responsabilidad del fabricante en base a su nivel de conocimiento efectivo y, por tanto, en base a la «culpa» del mismo.

Por último, un tercer grupo de circunstancias de exoneración afectan a la intervención de terceros o a la culpa exclusiva de la víctima.

En relación a la intervención de terceros, el art. 13 DRPD establece que «sin perjuicio de lo que indique el Derecho nacional en cuanto al derecho de repetición, los Estados miembros garantizarán que la responsabilidad de un operador económico *no* se reduzca o anule cuando los daños sean causados tanto por el carácter defectuoso de un producto como por acto u omisión de un tercero».

Para la intervención de un tercero que se suma al carácter defectuoso del producto, el art. 13.1 DRPD establece un régimen de responsabilidad directa del operador económico, basado en la defectuosidad del producto, sin perjuicio de la posibilidad de repetir contra el tercero que, con su conducta, haya producido una agravación del daño. Debe observarse que, en este caso, a pesar de que en el texto definitivo de la Directiva se haya añadido el término «anule», no puede producirse una exoneración de la responsabilidad del operador económico por la intervención de un tercero, en tanto que el producto es defectuoso y debe probarse o presumirse la relación de causalidad entre el daño y la defectuosidad del producto.

En cambio, respecto a la culpa exclusiva de la víctima, el art. 13.2 DRPD sí que contempla la posibilidad de «reducir o anular» la responsabilidad cuando el daño sea causado «conjuntamente por un defecto del producto y por culpa de la persona perjudicada o de una persona de la que la persona perjudicada sea responsable». Al contrario de lo que ocurre en el supuesto anterior, en este caso creemos que la posibilidad de «anular» la responsabilidad del operador económico en aquellos casos en los que el daño es causado «conjuntamente» por el carácter defectuoso del producto y por la actuación de la víctima (o de

¹⁵² NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019, p. 41.

las personas de las que sea responsable) resulta errónea, en tanto que sólo la ruptura del nexo causal entre la actuación del operador económico y el perjudicado por el daño, puede exonerar de responsabilidad al primero, y dicha ruptura no puede producirse cuando el daño deriva, en parte, del carácter defectuoso del producto. Por tanto, en este caso, lo que procedería igualmente es la moderación de responsabilidad.

Para solucionar estas cuestiones, la DRPD podría haber aludido a la exoneración de responsabilidad en aquellos supuestos en los que el daño fuera debido exclusivamente a la actuación de un tercero que queda fuera del control del operador económico o a la actuación del propio perjudicado por el daño, o de las personas de las que el perjudicado sea responsable. De esta forma, se hubieran distinguido claramente los supuestos de moderación de responsabilidad, de aquellos de exoneración de la misma.

3.3.2. Responsabilidad subjetiva o por culpa

A la luz de cuanto acabamos de exponer, la aplicación de un régimen de responsabilidad extracontractual subjetiva o por culpa al ámbito de los productos y servicios a los que nos referimos en el presente trabajo quedará limitada a dos supuestos:

En primer lugar, a aquellos casos en los que haya transcurrido el plazo de caducidad (sic. garantía) establecido en el art. 17 DRPD. En efecto, dicho precepto obliga a los Estados miembros a garantizar que el perjudicado deje de tener derecho a indemnización «conforme a la presente Directiva» cuando hayan transcurrido los plazos de diez o veinticinco años establecidos en el propio precepto sin que el perjudicado haya incoado, entre tanto, un procedimiento contra un operador económico que pueda ser considerado responsable. Pero lo que no dice es que, transcurrido ese plazo, no pueda reclamarse responsabilidad conforme a las reglas generales de cada estado miembro que, en nuestro caso, conducirían a las reglas generales de los arts. 1902 y ss. del CC.

En segundo lugar, respecto de aquellos casos en los que no podamos hablar de «productos» en sí mismos considerados o de «integrantes» de un producto, conforme a los criterios establecidos en la DRPD., supuesto que resulta especialmente importante en los casos de sistemas de inteligencia artificial.

Como se ha señalado en la doctrina¹⁵³, de los tres posibles tipos de responsabilidad subjetiva, a saber, responsabilidad por hecho propio, responsabilidad por hecho ajeno, y responsabilidad por hecho de las cosas, el que encaja

¹⁵³ PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva...” cit., p. 10.

mejor para imputar a los operadores económicos los daños derivados de la inteligencia artificial, es el sistema de responsabilidad subjetiva por el hecho de las cosas, dada la calificación de «cosa o bien» que podemos aplicar a los sistemas de inteligencia artificial.

Además, la aplicación de reglas de responsabilidad por culpa en el ámbito de la inteligencia artificial conlleva la ventaja de ir asociada al establecimiento de determinados deberes de conducta que, de ser seguidos por los sujetos, implicarán su diligencia¹⁵⁴; pero, por el contrario, conlleva la dificultad de aportar la prueba de la culpa o negligencia¹⁵⁵ habida cuenta de las características de los sistemas inteligentes¹⁵⁶:

- La *complejidad* de los sistemas que conlleva la interactuación de varios sujetos en su diseño y puesta en funcionamiento, complicando la determinación del grado de participación que cada uno de ellos pueda haber tenido en la causación jurídica del daño.
- La *autonomía* o capacidad del sistema para aprender por sí mismo. Precisamente, se ha dicho que uno de los factores esenciales, sino el «factor esencial» a la hora de definir un sistema de IA como de alto o de bajo riesgo es el grado de autonomía en su actuación a partir de la toma de decisiones, teniendo reflejo necesariamente en el régimen de responsabilidad civil al que se someta el operador¹⁵⁷.
- La *opacidad* o falta de transparencia, que impide conocer las instrucciones, factores o criterios en los que se basa la solución aportada por el algoritmo y su proceso de aprendizaje. Esta característica, que deriva, precisamente, de la capacidad del sistema de aprender con au-

¹⁵⁴ ATIENZA NAVARRO, M.L.: “La responsabilidad civil...”, cit., pp. 5-6. La especificidad de las conductas producidas en este ámbito hace prever que tengan que manejarse cánones de diligencia debida también específicos. En este sentido, PLATERO ALCÓN, A.: “Breves notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix”, *Ius et Scientia*, 2021, vol. 7, n° 1, <https://dx.doi.org/10.12795/IETSCIENTIA>, p. 151.

¹⁵⁵ Numerosos autores hablan de la dificultad de probar la «relación de causalidad», lo cual no es sino consecuencia del doble entendimiento de la causalidad como «causalidad física», que tiene por objeto identificar si la conducta o actividad de quien ha actuado ha dado lugar al daño sufrido por la víctima; y la «causalidad jurídica» como criterio de imputación o alcance de responsabilidad. Sobre ello vid. EVANGELIO LLORCA, R.: “Causalidad y responsabilidad civil por daños causados por sistemas de inteligencia artificial: las presunciones de causalidad y las propuestas normativas de la UE», Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora), pp. 5 y ss.

¹⁵⁶ ATIENZA NAVARRO, M.L.: “La responsabilidad civil...”, cit., pp. 2-3.

¹⁵⁷ NAVAS NAVARRO, S.: *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022, pp. 45 y 46.

tonomía¹⁵⁸, dificulta la imputación al hacer extremadamente difícil determinar quién controla el riego asociado al sistema de IA que está en el origen de la decisión que causa el daño¹⁵⁹, así como la prueba de la relación causal, habida cuenta de la complejidad y opacidad de la tecnología¹⁶⁰.

- La *imprevisibilidad* respecto de las decisiones adoptadas, derivada de la capacidad de aprendizaje, la autonomía y el grado de opacidad o falta de transparencia del sistema.
- La *conectividad* o intercambio continuo de datos con otros sistemas o dispositivos, y el sometimiento a actualizaciones y mejoras, lo que dificulta, de nuevo, la determinación de la causa del daño.
- La *vulnerabilidad* o sometimiento a ataques externos que pueden producir daños a quienes los utilicen.

En este sentido, la PDRIA no ha seguido la fórmula del RLIA, distinguiendo el fundamento de la responsabilidad civil, objetivo o subjetivo, en función del riesgo generado por el sistema, sino que implanta un sistema de responsabilidad subjetiva, con el fin de indemnizar por cualquier tipo de daño, también los derivados de un funcionamiento normal, y a cualquier tipo de víctima, pero aligerando la carga de la prueba mediante el establecimiento de presunciones refutables (*iuris tantum*) y estableciendo la posibilidad de obtener información sobre los sistemas de IA de alto riesgo, a favor de quienes soliciten una indemnización por los daños causados por sistemas de IA¹⁶¹.

¹⁵⁸ GIL MEMBRADO, C.: “Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra”, Ponencia presentada a las XII Jornadas de la APDC, Granada, octubre-2023 (versión pdf cedida por la autora), p. 8.

¹⁵⁹ PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva...”, cit., p. 12.

¹⁶⁰ ATAZ LÓPEZ, J.: “Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial”, *Càtedra Jean Monnet Working Paper*, 4/2020, <http://hdl.handle.net/2445/169850>, p. 31.

¹⁶¹ La propia exposición de motivos de la propuesta de Directiva reconoce que varios ordenamientos jurídicos nacionales prevén diferentes regímenes de responsabilidad objetiva y que, en su Resolución de propia iniciativa de 20 de octubre de 2020, el Parlamento Europeo también propuso elementos para un régimen de este tipo a escala de la UE, consistentes en un régimen de responsabilidad objetiva limitada para determinadas tecnologías basadas en la IA y en una carga de la prueba facilitada en virtud de normas de responsabilidad subjetiva. Las consultas públicas también pusieron de relieve la preferencia por un régimen de este tipo, a excepción de las grandes empresas que, cuando fueron cuestionadas sobre cambios de mayor alcance, como una inversión de la carga de la prueba o una presunción irrefutable (*iuris et de iure*), respondieron de forma negativa, eligiéndose, al final, medidas específicas para aligerar la carga de la prueba en forma de presunciones refutables, por tratarse de medios pragmáticos y adecuados para ayudar a las víctimas a soportar la carga de la prueba de la manera más específica y proporcionada posible. Además, la Comisión Europea añade como motivo el hecho de que los sistemas de alto riesgo, que son los que pueden provocar mayores daños a un gran número de personas, no están todavía extendidos en la actualidad.

No obstante, se trata de una solución provisional ya que, a tenor del art. 5 PDRIA, la implantación del régimen de responsabilidad civil será escalonada o por fases: en una primera fase, que durará cinco años desde su aprobación, únicamente se establece, para los sistemas de alto riesgo, la obligación de exhibición de pruebas y un sistema de presunciones *iuris tantum* y no *iuris et de iure*; por el contrario, en la segunda fase, una vez transcurridos los primeros cinco años, tendrá que procederse a una nueva evaluación del sistema de responsabilidad civil, a la vista de los cambios tecnológicos y de los siniestros habidos, decidiendo sobre la necesidad de introducir una responsabilidad de tipo objetivo, acompañada de un seguro obligatorio.

En relación al sistema propuesto durante los primeros cinco años de vigencia, el artículo 3.1 de la PDRIA establece que un órgano jurisdiccional puede ordenar la exhibición de pruebas pertinentes relativas a sistemas de IA de alto riesgo específicos de los que se sospeche que han causado daños. Las solicitudes de pruebas se dirigen al proveedor de un sistema de IA, a una persona sujeta a las obligaciones del proveedor establecidas en el artículo 24 o el artículo 28.1 de la PLIA, o a un usuario con arreglo a la PLIA. Las solicitudes deben estar respaldadas por hechos y pruebas suficientes para acreditar la viabilidad de la demanda por daños y perjuicios prevista y las pruebas solicitadas deben estar a disposición de los destinatarios. Las solicitudes no pueden dirigirse a partes que no estén sujetas a obligaciones en virtud de la PLIA y que, por tanto, no tengan acceso a las pruebas.

De conformidad con el artículo 3.4, párrafo primero, de la PDRIA el órgano jurisdiccional únicamente puede ordenar dicha exhibición en la medida necesaria para sustentar la demanda, dado que la información podría constituir una prueba fundamental para la demanda de la persona perjudicada en caso de daños en los que hayan mediado sistemas de IA. Al limitar la obligación de exhibición o conservación a las pruebas necesarias y proporcionadas, el mencionado precepto pretende garantizar la proporcionalidad en la exhibición de las pruebas, es decir, limitar la exhibición al mínimo necesario e impedir solicitudes genéricas.

Por último, el art. 3.5 contiene la presunción de incumplimiento por parte del demandado de su deber de diligencia pertinente, cuando incumpla la orden de un órgano jurisdiccional nacional de exhibir o conservar las pruebas que obran en su poder con arreglo a los apartados 1 o 2 del mismo precepto, asistiendo al demandado el derecho de refutar esa presunción.

Según expone la propia PDRIA, las medidas previstas en la misma «pueden encajar sin problemas en los sistemas de responsabilidad civil en vigor, ya que reflejan un enfoque que no depende de la definición de conceptos fundamentales como “culpa” o “daño”, dado que el significado de estos conceptos

varía considerablemente entre los Estados miembros de la UE». Así pues, más allá de las presunciones que establece la PDRIA, su regulación no afecta a las normas de los diferentes Estados que determinan, por ejemplo, qué parte ha de soportar la carga de la prueba, qué grado de certeza es necesario para que haya fuerza probatoria o cómo se define la culpa¹⁶².

En lo referente a la relación de causalidad, la PDRIA parte de la dificultad, por parte del demandante, para probar que existe un nexo causal entre el incumplimiento (*presunto*) y la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA que haya dado lugar a los daños en cuestión¹⁶³. En consecuencia, el art. 4.1 establece una presunción *iuris tantum* de causalidad específica en relación con este nexo causal entre la culpa del demandado y los resultados producidos por el sistema de IA, siempre y cuando se cumplan *todas* las condiciones siguientes:

- a) que el demandante haya demostrado o el órgano jurisdiccional haya supuesto, de conformidad con el artículo 3.5, la culpa del demandado o de una persona de cuyo comportamiento sea responsable el demandado, consistente en el incumplimiento de un deber de diligencia establecido por el Derecho de la Unión o nacional destinado directamente a proteger frente a los daños que se hayan producido;
- b) que pueda considerarse «razonablemente probable», basándose en las circunstancias del caso, que la culpa ha influido en los resultados producidos por el sistema de IA o en la no producción de resultados por parte del sistema de IA;
- c) que el demandante haya demostrado que la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA causó los daños, es decir, que exista relación de causalidad entre la actuación (o no actuación) de la IA y el daño.

De las tres condiciones expuestas, la única que supone una novedad respecto de las reglas generales del régimen de responsabilidad civil subjetiva es la segunda, ya que supone una rebaja en el estándar probatorio que se exige al demandante que ya no tendrá que probar que el daño era «previsible y evitable» habiendo utilizado la debida diligencia, sino que habrá de probar que es

¹⁶² Cfr. Exposición de Motivos Propuesta de Directiva sobre responsabilidad civil en materia de IA.

¹⁶³ Tal y como se ha dicho, en este sentido, para el autor de la propuesta este es el problema fundamental que plantea la aplicación del régimen subjetivo de responsabilidad a la IA. PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva...”, cit., p. 36.

«razonablemente probable» que la conducta del demandado haya influido en el resultado dañoso producido por el sistema de IA¹⁶⁴.

En el caso de las demandas por daños y perjuicios relacionadas con sistemas de IA que no sean de alto riesgo, la presunción de causalidad sólo se aplicará cuando el órgano jurisdiccional nacional considere «excesivamente difícil para el demandante demostrar el nexo causal» (art. 4.5). Además, el demandante siempre tendrá que demostrar que el sistema de IA (es decir, su información de salida o la no producción de una información de salida) ha causado los daños¹⁶⁵.

Así pues, la «probabilidad razonable» constituye el criterio conforme al cual el juez debe reconstruir la justificación de la decisión probatoria. No obstante, en los supuestos de daños derivados de sistemas de IA, dicho criterio sigue planteando inconvenientes, dado que, el grado de confirmación de una hipótesis aumenta o disminuye en función de los siguientes elementos¹⁶⁶: el *fundamento científico de las leyes causales* que conectan las pruebas con la hipótesis, que, en los casos de daños derivados de sistemas de IA, no es todavía sólido; la *solidez epistemológica (o el grado de certeza)* de las pruebas que la confirman, que, de nuevo, presenta dificultades dadas las características de los sistemas de IA a las que hemos hecho referencia; el *número de pasos inferenciales* que separan las pruebas de la hipótesis, ya que, en la mayoría de ocasiones, la hipótesis no vendrá confirmada por pruebas directas; y, por último, *la cantidad y variedad de pruebas o confirmaciones*, que dependerá también de las características de los sistemas de IA.

A continuación, los apartados 2 y 3 del art. 4 distinguen entre, por una parte, las demandas interpuestas contra el proveedor de un sistema de IA de alto riesgo o contra una persona sujeta a las obligaciones del proveedor en virtud de la PLIA y, por otra parte, las demandas interpuestas contra el usuario de dichos sistemas. A este respecto, siguen las disposiciones respectivas y las condiciones pertinentes de la PLIA. En el caso de las demandas fundadas en el artículo 4, apartado 2, el cumplimiento por parte de los demandados de las obligaciones enumeradas en dicho apartado debe evaluarse también a la luz del sistema de gestión de riesgos y sus resultados, es decir, las medidas de gestión de riesgos, con arreglo a la PLIA.

¹⁶⁴ PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva...”, cit., p.38.

¹⁶⁵ Sobre estas restricciones se ha dicho que ponen de manifiesto el limitado compromiso de la UE con las víctimas, sobre todo teniendo en cuenta que lo que hace que la prueba sea difícil no es el nivel o la intensidad del riesgo creado por el sistema de IA, sino el modo autónomo, opaco e impredecible con el que opera. PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva...”, cit., p. 40.

¹⁶⁶ GASCÓN ABELLÁN, M.: “Sobre la posibilidad de formular estándares de prueba objetivos”, *DOXA, Cuadernos de Filosofía del Derecho*, 28 (2005). p. 138.

Por último, la Propuesta de Directiva establece una excepción a la presunción de causalidad, cuando el demandado demuestre que el demandante puede acceder razonablemente a pruebas y conocimientos especializados suficientes para demostrar el nexo causal (art. 4.4) y otorga al demandado el derecho a refutar la presunción de causalidad (art. 4.7).

BIBLIOGRAFÍA

- ALKORTA IDIAKEZ, I.: *El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Aranzadi, Pamplona, 2022.
- ARNAU RAVENTÓS, L.: “Remedios por falta de conformidad en contratos de compraventa y de suministro de elementos digitales con varias prestaciones”, *Cuadernos de Derecho Transnacional* (Marzo 2020), Vol. 12, Nº 1, pp. 796 y ss.
- ARROYO Y AMAYUELAS, E.: “La propuesta de Directiva relativa a determinados aspectos de los contratos de compraventa en línea y otras ventas de bienes a distancia”, *Indret*, 3/2016.
- ATAZ LÓPEZ, J.: “Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial”, *Càtedra Jean Monnet Working Paper*, 4/2020, <http://hdl.handle.net/2445/169850>
- ATIENZA NAVARRO, M.L.: “¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)”, *Indret*, 2.2023.
- “La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora).
- BULLARD GONZÁLEZ, A.: “Causalidad probabilística: El problema de los costos administrativos en el diseño de un sistema de responsabilidad civil extracontractual”, *Ius et Veritas*, 1991, 2(3), pp. 3 y ss. Recuperado a partir de <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15312>
- CÁMARA LAPUENTE, S.: “El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015”, *InDret*, 3/2016, pp. 2 y ss.
- CARRASCO PERERA, A.; CORDERO LOBATO, E.; MARTÍNEZ ESPÍN, P.: “Transposición de la Directiva comunitaria sobre venta y garantías de los bienes de consumo”, *Estudios sobre consumo*, nº 52, 2000, p. 125 y ss.
- EBERS, M.: “Terapia sin terapeutas?”, en LUQUIN BERGARECHE, R. (Dir.): *Servicios privados de telemedicina y Salud Digital: retos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2023, pp. 32 y ss.

- EVANGELIO LLORCA, R.: “Causalidad y responsabilidad civil por daños causados por sistemas de inteligencia artificial: las presunciones de causalidad y las propuestas normativas de la UE», Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora).
- GASCÓN ABELLÁN, M.: “Sobre la posibilidad de formular estándares de prueba objetivos”, *DOXA, Cuadernos de Filosofía del Derecho*, 28 (2005). pp. 128 y ss.
- GIL MEMBRADO, C.: “Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora).
- GSELL, B. Y RODRIGO ARALDI, LL. M.: “Plazos de las medidas correctoras en caso de vicios ocultos según la Directiva (UE) 2019/770 sobre contratos de suministro de contenidos y servicios digitales y la Directiva (UE) 2019/771 sobre el contrato de compraventa de bienes”, *Cuadernos de Derecho Transnacional*, Octubre, 2020, vol. 12, nº 2, pp. 475 y ss.
- JORQUÍ AZOFRA, M.: *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023.
- LANDA REZA, I.: *El consentimiento de la persona mayor con discapacidad para el tratamiento de sus datos relativos a la salud*, Atelier, Barcelona, 2023.
- LUQUIN BERGARECHE, R.: “Responsabilidad contractual por el uso de la IA en la prestación de servicios de telemedicina y aplicaciones de salud digital”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por la autora).
- MACANÁS, G.: “Mutualización de los riesgos generados por los sistemas de IA”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por el autor).
- MARCOS GARCÍA, M.D.; RAMOS GONZÁLEZ, V.: *La administración segura de medicamentos en los nuevos escenarios electromagnéticos de Internet de las cosas (IoT)*, Madrid, Instituto de Salud Carlos III, Unidad de Investigación en Telemedicina y e-salud, 2018.
- MARÍN LÓPEZ M.J.: “Comentario al art. 116”, en R. BERCOVITZ RODRIGUEZ-CANO (COORD.), *Comentario del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*, Thomson Reuters, Pamplona, 2009.
- MARTÍNEZ VELENCOSO, L.M.: *La falta de conformidad en la compraventa de bienes*, Bosch, Barcelona, 2007.
- MÉNDEZ GARCÍA, M. Y RODA FAURA, M.: “Aproximación práctica al uso de las tecnologías big data en el sector salud”, *DS (Derecho y Salud)*, nº Extra 1, 2017 (Ejemplar dedicado al XXVI Congreso de Derecho Sanitario y Ciudadanía Europea: los retos), pp. 152 y ss.
- MONTEAGUDO PEÑA, J.L.: “La e-Salud en el marco de la Unión Europea. Aspectos organizativos, legislativos y operacionales”, <https://www.clubgertech.com/wp-content/uploads/2019/09/La-e-Salud-en-el-marco-de-la-UE.pdf>

- NAVAS NAVARRO, S.: “Salud electrónica e inteligencia artificial”, en S. Navas Navarro (Dir.) *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid 19)*, Comares, Granada, 2021, pp. 1 y ss.
- “Salud móvil”, en S. Navas Navarro (Dir.) *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid 19)*, Comares, Granada, 2021, pp. 51 y ss.
- *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022.
- NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019.
- ORTIZ FERNÁNDEZ, M.: “El derecho de daños ante la inteligencia artificial: la intervención de la Unión Europea”, *Actualidad Jurídica Iberoamericana*, n° 18, febrero 2023, pp. 1296 y ss.
- PEÑA LÓPEZ, F.: “Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la inteligencia artificial (provisional 03/10/23)”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por el autor).
- PLATERO ALCÓN, A.: “Breves notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix”, *Ius et Scientia*, 2021, vol. 7, n° 1, <https://dx.doi.org/10.12795/IETSCIENTIA>
- RUBÍ PUIG, A.: “Inteligencia artificial y daños indemnizables”, Ponencia presentada a las *XII Jornadas de la APDC*, Granada, octubre-2023 (versión pdf cedida por el autor).
- SÁNCHEZ LERÍA, R.: “Mercado digital y protección del consumidor: a propósito de la Directiva 770/2019 y su transposición al ordenamiento jurídico español”, *InDret*, 4.2021, pp. 33 y ss.
- TORRELLES TORREA, E.: “Telemedicina y pacientes vulnerables”, en AA.VV.: *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, 2023, pp. 165 a 181.

Interfaces cerebro-computador: protección de los neurodatos a través de los neuroderechos y de la responsabilidad civil del art. 82 del RGPD

MARÍA REMEDIOS GUILABERT VIDAL

*Prof.^a Ayudante Doctora
Universidad Miguel Hernández
(Acreditada a Prof.^a T.U.)*

Sumario: 1. Introducción. 1.1. El estado actual de la Neurotecnología: avances y desafíos. 1.2. Las interfaces cerebro-computador. 1.2.1. Concepto, tipos y funcionamiento. 1.2.2. Aplicaciones. 2. La protección dispensada por los neuroderechos. 2.1. Los neuroderechos como nuevos derechos fundamentales: Concepto y clases. 2.2. *Soft law* público y avances legislativos. 2.2.1. La Carta español de derechos digitales. 2.2.2. La regulación pionera de Chile. 3. Protección dispensada a los neurodatos por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. 3.1. Concepto y naturaleza jurídica del neurodato. 3.2. Responsabilidad por daños causados por infracción del derecho a la protección de datos en el ámbito de las *Brain Computer Interfaces* (BCI). 3.2.1. Sujetos. 3.2.2. Requisitos exigidos. A) Infracción. B) Daño. C) Relación causal. Bibliografía.

1. INTRODUCCIÓN

1.1. EL ESTADO ACTUAL DE LA NEUROTECNOLOGÍA: AVANCES Y DESAFÍOS

En una primera aproximación al estado actual de la Neurotecnología, deviene necesario realizar, con carácter previo, algunas precisiones termi-

nológicas. Así las cosas, debemos comenzar por la conceptualización de la Neurociencia¹. El saber neurocientífico se configura como una ciencia transversal que se ocupa del sistema nervioso o de cada uno de sus aspectos y funciones especializadas². Si bien, diversos autores ponen el acento en el estudio del cerebro y su incidencia en el comportamiento humano³. A su vez, en el seno de la Neurociencia también podemos distinguir, entre otras tantas disciplinas como la Neurología, Neuroanatomía, Neurofisiología, Neurohistología, Neurocirugía, etc.⁴. Por lo que se refiere en concreto a la Neurotecnología, ésta se remitiría a los diversos métodos e instrumentos que permiten la conexión directa de dispositivos técnicos con el sistema nervioso⁵.

En relación con el tema que nos ocupa, debemos hacer referencia obligada a la pionera STS (Sala de lo Penal, Sección 1ª), de 5 de mayo de 2020. En esta resolución se valoró el alcance de la prueba neurológica aportada, como fundamento de la imputabilidad de un condenado por asesinato. Resulta de notable interés el pasaje en el que el Alto Tribunal expone que «No falta razón a la defensa cuando subraya la importancia -no entendida por algunos- de una prueba tan certera como el PET-TAC para conocer el alcance de cualquier alteración neurológica. El papel de la neurociencia ha resucitado en la dog-

¹ Un sector de la doctrina sitúa a RAMÓN Y CAJAL como el precursor de esta disciplina, mientras que otra parte lo residencia en los años sesenta o incluso setenta del pasado siglo a raíz de las investigaciones realizadas sobre este campo en los Estados Unidos. Así, El *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, Oficina de Ciencia y Tecnología del Congreso de los Diputados, 2023, p. 1, manifiesta que las bases fundacionales de la Neurociencia fueron establecidas por RAMÓN Y CAJAL. Destacan por otro lado la corta vida de esta disciplina VARGAS MENDOZA, M.I./MANRIQUE MOLINA, F.E.R. Y YÁÑEZ NÚÑEZ, L.: “Neurociencia y Derechos Humanos: rama del bioderecho para fundamentar el derecho”, *Bioderecho.es*, núm. 15, enero-junio, Centro de Estudios en Bioderecho, ética y Salud, Universidad de Murcia, 2022, p. 5 y señala el año 1970 como origen institucional de la Neurociencia, a fundarse en esa fecha la *Society for Neuroscience* NARVAEZ MORA, M.: “Neuroderecho: el sentido de la acción no está en el cerebro”, *Revista de Teoría del Derecho de la Universidad de Palermo*, años 1, núm. 2, noviembre, 2014, p. 129.

² <https://dle.rae.es>, revisado el 17.7.2024.

³ En este sentido REGUERA ANDRÉS, M.C. Y CAYÓN DE LAS CUEVAS, J.: “La garantía de los neuroderechos: a propósito de las iniciativas emprendidas para su reconocimiento”, *Derecho y Salud*, vol. 31 (extraordinario), p. 214; ARAYA-PIZARRO, SEBASTIÁN C. Y ESPINOZA PASTÉN, L.: “Aportes desde las neurociencias para la comprensión de ellos procesos de aprendizaje en los contextos educativos”, *Propósitos y representaciones*, 2020, vol. 8, núm. 1, e312, p. 3, revisado el 17.7.2024.

⁴ En relación con el abuso de otros pretendidos neurosaberes, véase CORREDOR, K. y Cárdenas, F.P.: “Neuro-lo que sea” inicio y auge de una neurociencia para el siglo XXI, *Revista Iberoamericana de Psicología*, vol. 49, núm. 1-3, 2017, pp. 89-90 y también RESTREPO, J.E.: “Los límites epistemológicos de las neurociencias: la falacia de las neuro-lo que sea”, *Revista de Psicología Universidad de Antioquía*, vol. 11 (2), 2019, pp. 201-224.

⁵ Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, 2023, p. 1. Esta definición se recoge también en el art. 1. a) del proyecto de la ley chilena n° de Boletín 13828-19. A su vez, podemos distinguir diferentes tipos de Neurotecnologías, tales como la Neuroimagen, la Neuroestimulación y el *Neurofeedback*.

mática penal el interés por ciertos perfiles criminológicos que, en una visión histórica que se creía ya superada, predisponían al delito. Hoy asistimos a lo que con acierto se ha llamado una “*revolución neurocientífica*”. Las neurociencias, valiéndose de renovados métodos de experimentación y neuroimagen, están permitiendo un análisis de la mente humana inimaginable hasta hace bien poco. Las tesis defendidas por algunos neurocientíficos, que niegan toda escisión entre la mente y el cerebro, hasta el punto de que la actuación consciente no sería sino una ínfima expresión de nuestra actividad cerebral, han servido para reabrir una controversia histórica, a saber, el determinismo como explicación de muchos de nuestros actos. Se ha dicho, por entusiastas defensores de esta perspectiva, que “*no hacemos lo que decidimos, sino que decidimos lo que vamos a hacer de todas maneras*”. Es cierto que estamos ante un debate todavía en ciernes y sobre el que la Sala no tiene necesidad de pronunciarse. Pero lo que parece fuera de toda duda es que tan censurable como menospreciar la aportación de expertos en neurociencia, es abordar con frivolidad y simpleza el determinismo de los procesos neuronales, interpretando su realidad como muestra de fatalismo. Si así lo hacemos, corremos el riesgo de avalar una degradación de la naturaleza humana que convierte al hombre en un “títere del destino”⁶.

El origen de la Neurotecnología se puede situar sobre las bases asentadas por BROCA en 1861, al descubrir lesiones cerebrales durante las autopsias que realizaba en personas con problemas en el habla⁷. En la actualidad, esta acepción se entiende en sentido amplio al exponerse que se trata de «(...) un conjunto de dispositivos y procedimientos empleados para el acceso, control, investigación, evaluación, manipulación y/o emulación de la estructura y funcionamiento de los sistemas neuronales presentes en animales, incluyendo los seres humanos (...)»⁸.

La trascendencia y virtualidad de los novedosos sistemas actuales reside en su capacidad, no sólo de monitorear la actividad cerebral, sino también de modificar el sistema nervioso y el funcionamiento del cerebro⁹. De esta forma encontramos técnicas que permiten medir la actividad cerebral a través

⁶ RJ 2020/960.

⁷ DE LEÓN BARRIOS, V.H.: *Neurotecnología: el futuro*, Universidad de San Carlos de Guatemala, 2022.

⁸ Disponible en <https://espanadigital.gob.es>, consultado el 20.8.2024. Dentro de la emulación de sistemas neuronales destacaremos la inteligencia organoide la cual pretende mediante superar las limitaciones de la computación basada en silicio mediante la combinación de BCI con cultivos celulares 3D de neuronas, sobre esta cuestión véase *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C), 2023, p. 3.

⁹ *Declaración sobre neurodatos*, Red Iberoamericana de Protección de Datos, 25 de septiembre de 2023, p. 1.

de métodos invasivos y no invasivos, pudiendo aportar los primeros una mayor calidad en los resultados obtenidos. Dentro de las técnicas no invasivas destacaremos la resonancia magnética funcional, la electroencefalografía y la magnetoencefalografía. Los dispositivos capaces de modular la actividad cerebral, resultan especialmente controvertidos pudiendo presentar también naturaleza invasiva, como la estimulación eléctrica profunda o no invasiva, siendo fiel exponente de este último supuesto la estimulación magnética transcraneal. En este orden de cosas destaca el *Neurofeedback*, destacaremos su finalidad, la cual posibilita el mantenimiento en el tiempo de los cambios realizados en el cerebro, mediante el enlazamiento de la lectura de la actividad cerebral con una respuesta, entrenando de esta manera al paciente a su propio cerebro para la mejora de su funcionamiento¹⁰.

En la actualidad estamos presenciando un desarrollo exponencial de las Neurociencias y de la Neurotecnología, favorecido también por la convergencia de otras tecnologías como es el caso de la Inteligencia Artificial (IA), *Big Data*, Realidad Virtual, Nanotecnología, etc.

Como fruto de esta propicia situación somos testigos de extraordinarios avances en este campo de conocimiento, de tal manera que escenarios que preveíamos quizás poder alcanzar en las próximas décadas, son en la actualidad una realidad tangible.

Así resulta de especial interés los logros alcanzados por la empresa Neuralink, la cual ha logrado implantar un chip en el cerebro de un humano conectado a una computadora para paliar afecciones neuronales¹¹. Si bien debemos destacar el notable grado de escepticismo que generó en la comunidad científica su anuncio dado que, de forma inusual, tal y como suele acontecer en casos semejantes, no se vio acompañado de ninguna publicación especializada al respecto¹².

¹⁰ Sobre esta cuestión véase *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C), 2023, p. 3. Al respecto conviene precisar que la neuroestimulación produce efectos a corto plazo y la neuromodulación a largo plazo, véase *EDPS TechDispatch* Agencia Española de Protección de Datos, 2024, p. 3.

¹¹ Así, como paradigma de esta situación queremos resaltar la presentación al mundo del vídeo de *Neuralink* en marzo de 2024. En este material audiovisual se muestra cómo un hombre aquejado de tetraplejía es capaz de jugar al ajedrez contra una computadora, siendo capaz de dominar el cursor del ordenador, y con ello el movimiento de las figuras, únicamente mediante su propio pensamiento, <https://m.youtube.com>

¹² En este sentido véase RUÍZ MARTÍNEZ, J.: “Neurólogos españoles ponen en duda el anuncio de Elon Musk: No es una publicación científica”, <https://cadenaser.com>, revisado el 25.7.2024. También suscitó esta investigación controversias al conocerse daños infligidos a un buen número de animales utilizados en las investigaciones de la interfaz en cuestión, extremo que fue corroborado por la referida empresa tecnológica, https://www.abc.es/ciencia/abci-empresa-elon-musk-admite-tuvo-sacrificar-ocho-monos-dispositivos-neuralink-202202151828_noticia.html

De igual manera, debemos añadir que estos dispositivos no siempre resultan eficaces, siendo ineficientes en un buen número de casos, pese al proceso de “alfabetización Interfaz Cerebro Computador (ICC)” al que se somete al usuario. Entre causas del fracaso en el uso de estas aplicaciones, la doctrina apunta hacia la notable variabilidad de las señales; la insuficiencia de información o la falta de adaptación de los protocolos utilizados por los dispositivos al aprendizaje humano¹³.

Ante este escenario consideramos que estos logros científicos obligan, cuando menos, a realizar una reflexión sobre el potencial de la actual Neurotecnología, así como sobre los retos y amenazas que entrañan estos hitos científicos y tecnológicos. En cuanto a los progresos que han alcanzado estas tecnologías, qué duda cabe que con ella se abre un esperanzador horizonte para el tratamiento de gravísimas dolencias o al menos, de momento, para la mejora de la calidad de vida de las personas afectadas. Este es el caso de patologías como tetraplejia u otras limitaciones severas de la movilidad y del habla; la ceguera; la sordera; el Parkinson; la ELA, etc.¹⁴.

También en el campo de la rehabilitación y tratamiento del dolor, se está abriendo paso este conocimiento, en especial por lo que se refiere a las tareas imaginarias utilizadas para la extracción de actividad cerebral y su efecto en la neuroplasticidad¹⁵.

Igualmente, debemos apuntar que estas tecnologías no cierran su campo de aplicación al ámbito sanitario, sino que también son susceptibles de mejorar las capacidades intelectivas y cognoscitivas de las personas. En este sentido, ya se apunta como objetivo por la empresa *Neuralink* la consecución de mejoras en relación con otras capacidades humanas, más allá el ámbito estrictamente terapéutico¹⁶.

¹³ ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J.: “Interfaces cerebro-computadora: conceptualización, retos de diseño e impacto social”, *Revista Mexicana de Bioingeniería Mecánica*, vol. 40, núm. 3, septiembre-diciembre, 2019, pp. 3-4.

¹⁴ Sobre esta cuestión véase Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, 2023, p. 5. En relación con la utilización de las BCI para el control del cursor, neuroprótesis y rehabilitación de extremidades, sensación auditiva, sintetizadores de voz y prótesis ópticas, así como de los problemas que suscitan véase XIAYING ZHANG/ZIYUE MA/HUAIJIN ZHENG/TONGKENG LI/KEXIN CHEN/XUN WANG/CHENTING LIU/LINXI XU/XIAOHANG WU/DUORU LIN Y HAOTIAN LIN: “The combination of brain-computer interfaces and artificial intelligence: applications and challenges”, *Annals of Transnational Medicine*, jun, 8 (11): 712, pp. 3-16.

¹⁵ ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J., *op. cit.*, p. 14.

¹⁶ La propia página *web* de *Neuralink* manifiesta que: “Nuestra misión crear una interfaz cerebral generalizada para restaurar la autonomía de aquellos con necesidades médicas no satisfechas hoy y liberar el potencial humano mañana” y “En el futuro, esperamos restaurar capacidades como la visión, la función motora y el habla y, eventualmente, ampliar la forma en la que experimentamos el mundo”, disponible en <https://neuralink.com>, revisado el 25.7.2024.

Ello significa que se podría facilitar con el uso de estas interfaces el procedimiento de aprendizaje, aumentar y manipular la memoria e incluso incrementar la capacidad de visión nocturna¹⁷.

Respecto de las amenazas que se ciernen sobre los derechos de las personas, destacaremos, en primer lugar, el poder no sólo de leer la mente, sino también de escribirla. Tanto los sistemas denominados *read out* como *written in*, o incluso la combinación de ambos procedimientos, requerirán un tratamiento diverso por parte del Derecho, dado que los intereses que pueden resultar conculcados difieren en ambas aplicaciones tecnológicas.

La primera de estas técnicas es capaz de recibir y registrar señales del cerebro y decodificarlas mediante algoritmos de manera que pueda deducirse la intención motora del sujeto, mientras que el segundo de estos procedimientos envía señales al cerebro mediante técnicas de estimulación. Resulta obvio, por ejemplo, que valores fundamentales tales como la autonomía personal o el libre albedrío, se verán afectados de diferente modo por parte de cada una de estas herramientas tecnológicas, cuya indemnidad puede verse seriamente comprometida con la utilización de la segunda de las técnicas descritas, destinadas a escribir la mente. Incluso debemos apuntar que los sistemas BCI al estar conectados a Internet presentan serias vulnerabilidades frente al *hackeo* o violaciones de seguridad remotos¹⁸. Como se puede apreciar, los dispositivos *read out*, al registrar la actividad cerebral, plantearían problemas especialmente en el ámbito de la privacidad de los datos¹⁹.

En segundo lugar, las interfaces de naturaleza invasivas, es decir aquellas que requieren para su implantación de un procedimiento quirúrgico, plantean cuestiones en relación con los daños por los defectos que puedan presentar estos dispositivos, tanto si ostentan una finalidad terapéutica como de mejora de las capacidades de sujetos sanos²⁰.

Como consecuencia, todo el abanico del sistema de tutela del derecho fundamental a la protección de datos personales debe ser revisado con la finalidad de analizar su adaptabilidad a las nuevas circunstancias tecnológicas.

¹⁷ Así lo explica la *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C), 2023, p. 8.

¹⁸ Han demostrado las vulnerabilidades de estos sistemas ARMENGOL-URPI, A./KOVACS, R. Y SARMA, S.E.: "Brain-Hack: Remotely Injecting False Brain-Waves with RF to take control of Brain Computer Interfaces", *CPSIoTSec'23*, noviembre, 26, 2023 pp. 53-66.

¹⁹ XIAO-YU Y BIN YE: "The functional differentiation of brain computer interfaces (BCIs) and its ethical implications", *Humanities & Social Sciences Communications*, 2023, pp. 2-5.

²⁰ Sobre los riesgos de implantar BCI invasivas XIAO-YU Y BIN YE., *op. cit.*, p. 2. En cuanto a los beneficios y riesgos de la estimulación cerebral profunda, incluso en la esfera psicosocial de la persona tratada, véase SCHERMER, M.: "Ethical issues in Deep brain stimulation", *Frontiers in integrative neuroscience*, mayo, vol. 5, art. 17, 2011, pp. 1-2.

Y del mismo modo, la protección de la vida e integridad física, la identidad personal o el libre albedrío frente a la utilización de la Neurotecnología, han de aparecer necesariamente y de manera prioritaria en la agenda de los legisladores contemporáneos.

1.2. LAS INTERFACES CEREBRO-COMPUTADOR

1.2.1. Concepto, tipos y funcionamiento

Las interfaces objeto de estudio se definen usualmente como “(...) un sistema que mide la actividad del Sistema Nervioso Central (SCN) y la convierte en salidas artificiales que reemplazan, restauran, mejoran y suplementan salidas naturales por parte del SCN (...)”²¹. Esta acepción no incluiría la virtualidad que ostentan estos dispositivos para influir en la configuración de la actividad cerebral y que desde nuestra opinión debe ser adicionada necesariamente para garantizar una mayor protección de las personas.

Una definición similar de las BCI (*Brain Computer Interfaces*) la encontramos en el art. 1 b) del proyecto de la Ley chilena n° de Boletín 13828-19, en virtud del cual se trataría de «un sistema electrónico, óptico o magnético que: i) Mide la actividad del sistema nervioso central y la convierte en una salida conectada a una máquina o computadora o ii) Genera una respuesta artificial que reemplaza, restaura, complementa o mejora la respuesta del sistema nervioso natural y, por tanto, modifica las interacciones en curso entre el sistema nervioso y su entorno externo o interno.

Asimismo, debemos apuntar que la falta de consenso científico conlleva, en ocasiones, a utilizar indistintamente los términos BCI y Neurotecnología, si bien la correlación cerebro-ordenador se pudo llevar a cabo a partir del desarrollo de programación computacional²². De ahí que, con acierto, un sector de la doctrina se refiera, por ejemplo, a las “nuevas neurotecnologías”, denotándose con ello el notable desarrollo que han experimentado en los últimos tiempos, cuyos actuales desafíos las han ubicado en el centro de las investigaciones²³.

Para una mejor precisión conceptual de las BCI, debemos, por tanto, hacer referencia a la diversa tipología existente de las mismas. Así, debemos

²¹ ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J., *op. cit.*, p. 4.

²² *Informe El desarrollo humanista de la neurotecnología, una nueva oportunidad para España*, Digital Future Society, 2024, nota n° 2, p. 12.

²³ YUSTE, R.: *Las nuevas neurotecnologías y su impacto en la ciencia, medicina y sociedad*, Lecciones Cajal, Universidad de Zaragoza, 2019, disponible en <https://puz.unizar.es>, consultado el 29.8.2024.

partir de la distinción realizada con anterioridad entre dispositivos destinados a la lectura de los impulsos cerebrales (*read out*), de aquellos otros cuya finalidad es provocar nuevos estímulos en el cerebro (*write in*). De este modo, se distinguen entre BCI unidireccionales, aquellos que actúan desde el cerebro hacia la computadora para detectar la actividad neuronal, o bien desde la computadora al cerebro para estimularlo. Y también de naturaleza bidireccional, es decir, funcionando en ambas direcciones²⁴.

La primera de estas técnicas mapea las señales cerebrales, las cuales se interpretan gracias a determinados algoritmos con el objeto de conocer la intención del usuario. Estos sistemas se componen usualmente de los siguientes elementos: usuario; EGG; procesador digital de señales; generador de características; traductor de características; sistema de control; retroalimentación; controladores; dispositivo o aplicación objetivo y monitor neuronal.

Por lo que respecta al funcionamiento de estas interfaces cerebro-computador, podemos distinguir los siguientes pasos. En primer término, se registra la actividad cerebral; en segundo lugar, se procesa la información; en tercer lugar, se extraen y seleccionan las características eléctricas; en cuarto lugar, utilizando algoritmos se reconocen patrones neuronales; en quinto lugar, se lleva a cabo la acción deseada por el usuario. Finalmente, también podemos hacer referencia a la retroalimentación o *feedback* que recibe el usuario de la acción desplegada²⁵.

En resumidas cuentas, encontramos unos sensores para registrar la actividad cerebral, un decodificador, es decir el algoritmo matemático y unos efectores como sería el caso de una extremidad robótica²⁶.

En este proceso ocupa un destacado papel el empleo de algoritmos para decodificar las señales captadas mediante la EEG, dado que con ello se da entrada a la convergencia de la Inteligencia Artificial con las BCI, incrementándose así considerablemente los desafíos planteados en el campo de la Neurotecnología²⁷.

²⁴ GARCÍA, L.V. Y WINICKOFF, D.E.: “Brain-computer interfaces and governance system: Upstream approaches”, *OECD Science, Technology and Industry Working Papers*, núm. 1, 2001., pp. 11-12.

²⁵ ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J., *op. cit.*, pp. 6-7.

²⁶ MONASTERIO ASTOBIZA, A./ AUSÍN, T./TOBOSO, M./MORTE FERRER, APARICIO PAYÁ, R, Y LÓPEZ, D.: “Traducir el pensamiento en acción: Interfaces cerebro-máquina y el problema ético de la agencia”, *Revista de Bioética y Derecho*, núm. 46, 2019, p. 31-32. Otros autores distinguen entre adquisición de la señal, procesamiento de la señal, en la cual se produce la extracción, clasificación y traducción de las características y la aplicación MAISELI B./ABDALLA, A. T./MASSAWE, L.V./MERCY MBISE/MKOCHA, K./NASSOR NASSOR, A./ISMAIL, M./MICHAEL, J. Y KIMAMBO, S.: “Brain-computer interface: trend, challenges and theats”, *Brain Informatics*, 10, 20, 2023, p. 2.

²⁷ Realiza un examen de un buen número de algoritmos destinados a la evaluación de los datos cerebrales recopilados mediante EGG GARCÍA HERRERO, C.A.: “Análisis de los algoritmos

En la actualidad encontramos infinidad de estos instrumentos con muy diversas funcionalidades, tales como el movimiento de extremidades, identificación de emociones, clasificación de imágenes motoras, sistemas ortográficos, detección de anomalías cerebrales, visión artificial, etc.

Esta variabilidad de aplicaciones obliga a tener muy presentes las disposiciones del Reglamento sobre Inteligencia Artificial de la Unión Europea (*Artificial Intelligence Act*), por ejemplo al proscribir en el art. 5 apartado 1, a), b), c) f) y g) la IA subliminar y manipuladora; la que explote vulnerabilidades; determinados sistemas de evaluación, clasificación o predictivos; también de perfilado a partir de biometría con datos especiales y aquellos que destinados al reconocimiento de emociones en entornos educativos y laborales.

Igualmente debemos indicar que estas interfaces cerebrales se suelen clasificar en activas, reactivas, pasivas e híbridas. En cuanto a los sistemas activos, debemos señalar que se controlan por el usuario, a través de tareas mentales utilizadas en el entrenamiento. De este modo podemos citar los movimientos imaginarios; la rotación mental de cuerpos en 3D; la lingüística mental o la musicalización interna.

Por su parte, los denominados como interfaces reactivas, obtienen los datos cerebrales a partir de estímulos aplicados sobre el usuario de tipo visual, auditivo, táctil u olfativo, sin necesidad de una especial preparación. Las aplicaciones pasivas, no controlan dispositivos y detectan estados de ánimo como ansiedad, fatiga, frustración o atención. Y finalmente, aquellas interfaces de carácter híbrido obtienen la actividad cerebral combinando bien interfaces activas y reactivas, bien diversas fuentes fisiológicas²⁸. También debemos hacer mención a la posibilidad de recolección, no sólo local, si no también remota de los neurodatos, dados los riesgos inherentes que presenta esta circunstancia²⁹.

Las segundas de las tecnologías enunciadas, es decir las denominadas *write in*, son capaces de estimular el cerebro mediante impulsos que pueden ser eléctricos o lumínicos³⁰.

De igual modo estos sistemas, puede utilizar algoritmos matemáticos de forma simultánea con la modulación cerebral, para de este modo ajustar con la máxima precisión el estímulo a la concreta área objeto de estimulación. Por

para la caracterización de señales cerebrales EGG", *Ingeniería electrónica*, Universidad Cooperativa de Colombia, Bogotá, 2021.

²⁸ Tipología de las ICC extraída de ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J., *op. cit.*, pp. 5-7.

²⁹ EDPS *TechDispatch* Agencia Española de Protección de Datos, 2024, p. 3.

³⁰ XIAO-YU Y BIN YE, *op. cit.*, p. 2.

otra parte, debemos recordar que, tanto los sistemas de lectura como los que modifican la actividad cerebral pueden ser catalogados como de naturaleza invasiva o no invasiva, dependiendo de la necesidad de intervención quirúrgica para introducirlos en la piel del usuario para hacer efectivo su funcionamiento, pudiéndose implantar en la corteza cerebral o entre el cerebro y la estructura ósea³¹.

De esta manera también se distinguen por la doctrina científica técnicas parcialmente invasivas, las cuales requieren de una mínima cirugía para ser implementados³².

Como resulta evidente, la utilización de la cirugía incrementa los riesgos sobre la integridad y salud del usuario. Los sistemas denominados *read out* no suelen ser de carácter invasivo, dado que utilizan técnicas como el electroencefalograma o imagen por resonancia magnética funcional, a diferencia de las interfaces *write in* basadas en la implantación de electrodos en determinadas áreas del tejido cerebral, como es el caso de la estimulación craneal profunda³³. Además, se requiere introducir un neuroestimulador, bien infraclavicular o abdominal, conectado mediante una extensión subcutánea al electrodo³⁴.

1.2.2. Aplicaciones

Tras el examen realizado, resultaría ingenuo pensar que el uso de los BCI se circunscribiese tan solamente a la consecución de finalidades terapéuticas. Los neurodatos ofrecen una ingente cantidad de información sin parangón sobre la persona, incluso de parcelas perteneciente al subconscientes y desconocidas por el propio usuario. Esta tecnología no sólo permite escrudiñar detalles sobre los gustos, aficiones, adicciones, enfermedades, tendencias, personalidad, etc., sino también la manipulación de las diferentes áreas cerebrales pudiendo con ello modificar la integridad mental, personalidad, conciencia de sí mismo y con ello el libre albedrío. El potencial de esta tecnología ha propiciado la existencia de avances científicos, en primer término, como hemos indicado con anterioridad, relacionadas con el ámbito sanitario y también de

³¹ MONASTERIO ASTOBIZA, A./ AUSÍN, T./TOBOSO, M./MORTE FERRER, APARICIO PAYÁ, R, Y LÓPEZ, D., *op. cit.*, p. 32.

³² GARCÍA, L.V. Y WINICKOFF, D.E., *op. cit.*, p. 10.

³³ XIAO-YU Y BIN YE, *op. cit.*, pp. 2-3.

³⁴ Explican con detalle el procedimiento para implantar esta técnica ESCOBAR VIDARTE, O.A./ OROZCO MERA, J. Y ORDÓÑEZ CASTILLO, J.A.: "Precisión en implantación de electrodos para estimulación cerebral profunda para el manejo de trastornos del movimiento", *Revista ELA*, año IX, vol. 19, edición núm. 37, enero-junio, 2022, p. 6.

los videojuegos, educación, usos militares e incluso concernientes al denominado mejoramiento personal (*enhancement*)³⁵.

La realidad virtual se configura como otro espacio en el que con toda probabilidad tendrán una incidencia significativa las BCI. La confluencia de estos dispositivos con otras tecnologías disruptivas en el seno del Metaverso, o mejor dicho metaversos, está llevando a cabo sus primeros y decisivos pasos. De este modo, en dicho entorno virtual podrán quedar residenciadas otras innovaciones tales como la Inteligencia Artificial, 6G, *Blockchain*, *Big Data*, etc., potenciándose con ello de forma exponencial las funcionalidades en esta nueva realidad digital. De este modo, el control de los avatares a través de la propia mente supondría una mejoría extraordinaria en relación a su usabilidad, así como también un mayor confort frente a los dispositivos tradicionales utilizados en la realidad virtual, como es el caso de las gafas o los cascos. Tanto la industria del videojuego, como el campo de la neurorrehabilitación o la terapia psicológica son campos en los cuales el potencial de las BCI podrá ser desarrollado³⁶. Igualmente, la utilización de la realidad virtual, por ejemplo, en los dispositivos destinados para la mejora de la movilidad facilitará el entrenamiento de los usuarios, al recibirse una retroalimentación multisensorial mucho más natural de las acciones ejecutadas. De este modo se incrementará significativamente la tasa de éxito en el uso de los dispositivos BCI³⁷.

2. LA PROTECCIÓN DISPENSADA POR LOS NEURODERECHOS

2.1. LOS NEURODERECHOS COMO NUEVOS DERECHOS FUNDAMENTALES: CONCEPTO Y CLASES

Tal y como se desprende de la investigación realizada, la tecnología objeto del presente estudio plantea un desafío sin precedentes en relación con la esfera más íntima de la personalidad del individuo, pudiéndose prever consecuencias irreversibles en los derechos más fundamentales de la persona. En este sentido, valores indispensables como la libertad, vida, integridad física y

³⁵ En el ámbito europeo, debemos subrayar por su trascendencia, que los usos militares se encuentran extramuros de la regulación del Reglamento Europeo sobre Inteligencia Artificial (*Artificial Intelligence Act*) con arreglo al art. 2.3 de esta norma.

³⁶ Sobre la relación de las BCI en la realidad virtual véase *Informe C: Avances en neurociencia: aplicaciones e implicaciones éticas*, Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C), 2023 p. 6.

³⁷ ALONSO-VALERDI, L.M./ARREOLA, M.A. Y ARGÜELLO GARCÍA J., *op. cit.*, p. 13.

moral, intimidación, igualdad, etc. son susceptibles de verse amenazados a causa de una utilización torticera de estas neurotecnologías. A este respecto resulta, cuando menos sorprendente, que la denuncia de esta situación haya venido precisamente de la mano de los expertos en Neurología y no por parte del ámbito jurídico, el cual, desde nuestra consideración está avanzando sin la prontitud deseable³⁸.

En este sentido resulta obligada referencia a la labor que han venido desempeñando el reconocido grupo multidisciplinar de estudiosos de la Universidad de Columbia, denominado *Morningside*, quien lleva años dedicados a la promoción y reconocimiento como derechos humanos de los denominados neuroderechos. En términos concisos, los neuroderechos se pueden conceptualizar como el conjunto de derechos humanos para proteger el cerebro³⁹.

En un principio se distinguieron por dichos investigadores diversas áreas en las que se requería una acción protectora prioritaria: privacidad y consentimiento; libre albedrío e identidad; aumento cognitivo y sesgos⁴⁰.

Con posterioridad, en el año 2021, el referido grupo estadounidense de académicos, expuso unos concretos neuroderechos, propugnándose además su inclusión en el vigente catálogo de derechos humanos. A saber: derecho a la identidad o control de la integridad física y mental; derecho a la libertad de pensamiento y libre albedrío; derechos a la privacidad mental; derecho al acceso justo a la mejora mental y derecho a la protección frente al sesgo algorítmico⁴¹. Otro sector de la doctrina, de forma más restrictiva, dando buena prueba de la falta de consenso en torno a la extensión de los neuroderechos, distingue como neuroderechos los que a continuación se esbozan: el derecho a la libertad cognitiva, el derecho a la privacidad mental, el derecho a la integridad mental y el derecho a la continuidad psicológica⁴².

³⁸ Encontrándonos con ello con un *softlaw* de origen privado, en este sentido REGUERA ANDRÉS, M.C. Y CAYÓN DE LAS CUEVAS, J.: "La garantía de los neuroderechos: a propósito de las iniciativas emprendidas para su reconocimiento", *Derecho y Salud*, vol. 31 (extraordinario), pp. 216.

³⁹ YUSTE, R./GENSER, J. Y HERRMANN, S.: "It's time for neurorights", *Horizons*, núm. 18, 2021, p. 160.

⁴⁰ YUSTE, R./GOERING, S./AGÜERA Y ARCAS, B./GUOQUIANG BI/ CARMENA, J.M./CARTER, A./FINS, J.J./FRIESEN, P./GALANTE, J./HUGGINGS, J.E./ILLES, J./KELLMAYER, P./KLEIN, E./MARBLESTONE, A./MITCHELL, C./PARENS, E./PHAM, M./RUBEL, A./NORIHIRO SEDATO/SPECKER SULLIVAN, L./TEICHER, M./WASSERMAN, D./WEXLER, A./WHITTAKER, M. Y WOLPAW, J.: "Four ethical priorities for neurotechnologies and IA", *Nature*, vol. 551, 2017, pp. 3-4.

⁴¹ YUSTE, R./GENSER, J. Y HERRMANN, S.: "It's time for neurorights", *Horizons*, núm. 18, 2021, pp. 160-161.

⁴² IENCA, M. Y ANDORNO, R.: "Hacia nuevos derechos humanos en la era de la neurociencia y neurotecnología", *Análisis Filosófico*, núm. 41, vol. 1, mayo 2021, p. 155. Otras posturas abogan por la positivización como derechos humanos, en el ámbito que nos ocupar, de los derechos de libertad

No obstante esta iniciativa, también han surgido voces contrarias al reconocimiento a nivel de derecho humano de los intereses expuestos. Estas posiciones se fundan, entre otras argumentaciones, en la perniciosa inflación de los derechos humanos, su indeterminación e incoherencia o la redundancia de la que adolecen respecto de los derechos humanos ya reconocidos en la actualidad⁴³.

De la misma manera, se han llegado a proponer, unas interesantes medidas para la protección de dichos intereses, configurándose algunas de ellas a corto plazo y otras con aplicación en el largo plazo. Así, entre las primeras, se ha destacado la necesidad de crear una definición de naturaleza consensuada acerca de los neuroderechos; en segundo lugar, el nombramiento por parte de la ONU de asesores para facilitar el marco regulatorio de los neuroderechos y un tratado internacional sobre los mismos y, en tercer lugar, la realización de consultas periódicas entre los Estados con programas avanzados en estas materias y la ONU. Como medidas de aplicación más diferida en el tiempo, se incidió en la creación de un tratado internacional o protocolo adicional para incorporar los derechos neurológicos; la adopción de Observaciones generales sobre neuroderechos; el nombramiento de un Relator especial que analizase el impacto de las neurotecnologías en los derechos humanos en la actualidad y finalmente, la creación de una agencia especializada en materia de neuroderechos⁴⁴.

2.2. SOFT LAW PÚBLICO Y AVANCES LEGISLATIVOS

2.2.1. La Carta española de derechos digitales y la Declaración de León

En el ámbito europeo, España se erige en como referente en cuanto a la promoción de los neuroderechos, si bien los esfuerzos, de momento, han cristalizado en un instrumento de carácter no vinculante, la denominada Carta española de derechos digitales del año 2021. Este documento, de contenido programático, recoge una serie de intereses individuales que han de ser ga-

(derecho a la identidad propia, derechos a la identidad de pensamiento y derechos a la privacidad mental), así como la protección contra el sesgo algorítmico y a que no se produzcan perjuicios en base a la neurotecnología, así BAJATIERRA RUÍZ, M.: “Una argumentación moral de los neuroderechos humanos”, *Revista Electrónica de Estudios Penales y de la Seguridad*, núm. 12, 2023, pp. 23-24.

⁴³ Sobre las críticas vertidas a la conceptualización de estos nuevos derechos humanos véase DE ASÍS, R.: “Sobre la propuesta de los neuroderechos”, *Derechos y libertades*, núm. 47, Época II, junio 2022, pp. 67-70.

⁴⁴ YUSTE, R./GENSER, J. Y HERRMANN, S.: “It’s time for neurorights”, *Horizons*, núm. 18, 2021, pp. 160 y 162-163.

rantizados por una la eventual legislación que se desarrolle en el ámbito de las neurotecnologías. Así en el apartado XXVI se hace referencia a conceptos como la propia identidad; la autodeterminación individual; confidencialidad y seguridad de los datos relativos a procesos cerebrales y pleno dominio sobre los mismos; regulación de las BCI capaces de afectar a la integridad o al suministro de datos sesgados para la adopción de decisiones. También en la Carta se observa la preocupación por el mejoramiento mental queda plasmado en el subapartado 2, en cuanto se aboga por garantizar la igualdad y no discriminación mediante la regulación del aumento cognitivo, la estimulación o potenciación de las capacidades personales, incluso más allá de las finalidades terapéuticas. Con ello se intentaría proteger el acceso a las equitativo a las neurotecnologías, si bien la prioridad y aplicación real de este derecho está en tela de juicio, tal y como hemos comentado con anterioridad⁴⁵.

Como se puede observar, el contenido recogido en la citada Carta coincide en lo sustancial con el contenido de los neuroderechos apuntados por la doctrina, a la que nos hemos referido con anterioridad. Si bien, como se aprecia, no se establece un reconocimiento expreso de nuevos neuroderechos fundamentales, sino que se limita a sugerir una política legislativa que ampare a las personas frente a los riesgos del empleo de la moderna Neurotecnología⁴⁶.

Por otro lado, y precisamente también en España, concretamente en la ciudad de León, se firmó en 2023 una Declaración en virtud de la cual los Estados firmantes, a través de sus ministros de comunicaciones, expresaron su intención de construir un espacio confiable para los consumidores frente a los riesgos de las neurotecnologías. Sobre este particular, resulta interesante la especial preocupación de dicho instrumento por los dispositivos no invasivos de libre uso entre los consumidores, si bien esta inquietud debiera haberse trasladado a todo tipo de BCI. De este modo, se expone que neurotecnologías ofertadas en la actualidad al público en general adolecen de un control suficiente frente a los eventuales perjuicios que puedan provocar en la salud o privacidad de los datos personales, cuyo mercado, dicho sea de paso, ha aumentado considerablemente en los últimos tiempos. Además, desde el punto de vista jurídico presenta un especial interés la industria del entretenimiento, dado que sus principales y más vulnerables actores son las personas menores⁴⁷.

⁴⁵ Véase sobre este particular la reflexión de BAJATIERRA RUÍZ, M.: “Una argumentación moral de los neuroderechos humanos”, *Revista Electrónica de Estudios Penales y de la Seguridad*, núm. 12, 2023, pp. 24.

⁴⁶ Sobre la naturaleza prospectiva de este texto véase REGUERA ANDRÉS, M.C. Y CAYÓN DE LAS CUEVAS, J., *op. cit.*, p. 216.

⁴⁷ Sobre esta cuestión véase SANZ DE GALDEANO, M.: “La Declaración de León sobre la neurotecnología europea: Un primer paso necesario”, *Diario la Ley*, Sección Ciberderecho, núm. 77, noviembre, 2023, disponible en <http://diariolaley.laleynext.es>, consultado el 22.8.2024.

Como colofón a la comentada Declaración, los Estados firmantes solicitan actuaciones tales como: fomentar la cooperación entre el sector público y privado; alimentar un ecosistema dinámico; considerar medidas de acompañamiento e inversión; facilitar debates de expertos; fomentar el diálogo entre la Comisión Europea y los Estados; obligar a los líderes de innovación a adherirse a un enfoque centrado en la persona; informar al público; crear un ecosistema confiable y estudiar la necesidad de crear normas⁴⁸.

2.2.2. La regulación pionera de Chile

Chile se sitúa a nivel mundial como un exponente en materia de protección de los neuroderechos a través del *hardlaw*. De este modo en dicho Estado se han llevado a cabo dos reformas legislativas esenciales. En primer lugar, la relativa a su Constitución, en virtud de la cual se modificó en 2021 el art. 19 n° 1, mediante el art. único de la Ley 21.383, el cual determina que “El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para la utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella”.

La regulación que finalmente se aprobó difirió sustancialmente de la contenida en el proyecto de ley de reforma constitucional, el cual se expresaba en los siguientes términos “La integridad física y psíquica permite a las personas gozar plenamente de su identidad individual y de su libertad. Ninguna autoridad o individuo podrá, por medio de cualquier mecanismo tecnológico, aumentar, disminuir o perturbar dicha integridad individual sin el debido consentimiento. Sólo la ley podrá establecer los requisitos para limitar este derecho, y los requisitos que debe cumplir el consentimiento en estos casos”.

Tras un procedimiento de reforma constitucional considerablemente complejo en el que resultó loable la participación de muy diversas opiniones científicas, se llegó como se puede observar con facilidad, a un resultado sustancialmente diferente al proyecto propuesto, circunstancia que bien merece las siguientes consideraciones. En primer lugar, se decidió obviar la referencia al consentimiento que se propuso en un primer momento. Este cambio se debió fundamentalmente a que el mismo resultaba ya reconocido,

⁴⁸ También debemos citar en este apartado la Declaración de Valencia sobre la incorporación de los neuroderechos en la Declaración universal de derechos humanos de 2023.

pudiendo incorporar más dudas que certezas mediante su inclusión en el texto constitucional⁴⁹.

En segundo lugar, se excluyeron términos complejos como identidad individual y libertad, en su vertiente de libre albedrío. En tercer lugar, se remitió a la ley para la determinación de los requisitos, condiciones y restricciones (términos prácticamente equivalentes), para la utilización del desarrollo científico y tecnológico en las personas, debiendo resguardar dicha ley la tanto la actividad cerebral como la información proveniente de ella.

En cuarto lugar, resulta de interés indicar que se conservó la referencia a valores tradicionales desde el punto de vista constitucional, esto es, la integridad física y mental, como elementos constitutivos de la identidad. A éstos se adicionó el respeto a la vida, la cual también, sin duda, está en riesgo frente a la utilización desviada de la Neurotecnología, siendo, no obstante, redundante su inclusión en este precepto.

En quinto lugar, tampoco estimó prudente al legislador constituyente chileno incluir que la ley fuese autorizada para limitar el derecho a la integridad física y psíquica. Quizás ello se debió a los riesgos de justificar la manipulación cerebral ilícita sobre la base, por ejemplo, de la tan manida seguridad. O incluso, por otra parte, se viese alterado su contenido por los vaivenes políticos.

En sexto lugar, resulta un tanto forzoso afirmar que el núcleo esencial del nuevo “derecho fundamental a la neuroprotección” finalmente aprobado, coincide con el establecido en el proyecto de reforma constitucional y que recogía la propuesta del *Morningside Group*. En el referido proyecto de reforma se indicaba que su contenido esencial englobaba el derecho a la privacidad de la información producida por la actividad cerebral; el derecho a la identidad personal y a la autodeterminación; el derecho a la igualdad frente al aumento de capacidad cerebral y derecho al control de sesgos de los algoritmos. Deviene con facilidad colegir que el texto constitucional aprobado recoge la protección a la identidad personal, al proteger la integridad psíquica, y la privacidad de los datos cerebrales. También incluso de forma implícita el libre albedrío al resguardar especialmente la actividad cerebral. No obstante, el acceso equitativo a las mejoras y la protección frente a los sesgos algorítmicos no aparecen en la redacción del precepto, si bien podrán derivarse del derecho a la igualdad. Igualmente, no podemos dejar de referirnos al acierto de la reforma al reconocerse la protección constitucional de la información

⁴⁹ Se muestra partidario a la redacción final de la reforma constitucional que excluye las dos menciones originarias al consentimiento MARZUCA ABUMOHOR, T.R.: *Neuroderecho: Análisis de la ley N° 21.383 (Boletín N° 13.827) y el Boletín N° 13.828 sobre neuroprotección e indemnidad mental*, Universidad de Chile, Santiago, 2023, p. 88, disponible en <https://repositorio.uchile.cl>, consultado el 22.8.2024.

y de la actividad cerebral tanto frente a las aplicaciones *read out*, como a las denominadas *write in*, si bien no contiene una prohibición de la utilización de éstas últimas cuando tengan, por ejemplo, como objetivo manipular la mente de las personas.

Tal y como hemos apuntado con anterioridad, en segundo término, resulta esencial destacar el proyecto de Ley chilena sobre protección de los neuroderechos y la indemnidad mental y el desarrollo de la investigación y las neurotecnologías, la cual se encuentra en tramitación en el momento de redacción de estas líneas. Esta ley pretende dotar de contenido la reforma constitucional abordada con anterioridad.

En relación con esta norma, tan solo destacar algunos de los aspectos de interés tratados en la misma, dado que un estudio exhaustivo de la misma desbordaría el objeto del presente estudio. De esta manera, el Proyecto de ley votado en Sala en Primer Trámite establece en el art. 1 los objetivos de la norma. Así expresamente se propone proteger la integridad física y psíquica de las personas mediante la protección de la privacidad de los neurodatos, del derecho a la autonomía y el acceso a la neurotecnología sin discriminaciones arbitrarias; fomentar la concordancia entre el desarrollo de las neurotecnologías con los principios éticos y garantizar la información a los usuarios sobre potenciales consecuencias negativas.

Mediante esta norma, podemos advertir que el legislador chileno va incorporando los principios del grupo *Morningside* de forma más explícita al ordenamiento jurídico chileno, con un contenido que amplía el establecido constitucionalmente.

Respecto de las medidas previstas en los artículos 3 y 4 para la protección de la integridad y privacidad mental, el texto se centra en la prohibición de cualquier intervención cerebral que no cuente con el consentimiento libre, expreso e informado de la persona, incluso cuando la tecnología pueda intervenir en ausencia de conciencia en circunstancias médicas. Asimismo, a diferencia de lo plasmado en la reforma constitucional, se prohíbe cualquier sistema de manipulación de la actividad neuronal que pueda dañar la continuidad psicológica y psíquica de la persona, identidad o autonomía. Esta previsión tendrá especial incidencia en relación con los dispositivos de estimulación cerebral profunda en la medida que puedan modificar aspectos de la personalidad de los pacientes, si bien resultará discutible el grado de afectación frente a los beneficios que pueda conllevar la terapia neurológica. En este sentido, como parámetro interpretativo, el proyecto determina que el límite para la intervención neuronal será la protección de los “sustratos mentales de la identidad personal”, los cuales no quedan desarrollados.

Por lo que respeta al formulario de solicitud del consentimiento para la aplicación del procedimiento neurológico, el art. 5 establece que se deberá indicar los efectos físicos, cognitivos y emocionales, derechos y deberes, normas sobre protección de datos, medidas de seguridad y contraindicaciones. Además, el art. 6 de la norma proyectada determina que los datos neuronales constituyen una categoría especial de datos sensible de salud, iniciativa que bien podría seguir el legislador europeo.

Finalmente, el art. 7 se remite a la Ley núm. 19.451 sobre trasplante y donación de órganos en cuanto le sea aplicable a la recopilación, almacenamiento, tratamiento y difusión de datos neuronales y actividad neuronal. De este modo, resulta de especial interés traer a colación el art. 3º de dicha norma en el que se determina que “La donación de órganos sólo podrá realizarse a título gratuito. Se prohíbe, será nulo y sin ningún valor el acto o contrato que, a título oneroso, contenga promesa o entrega de un órgano para efectuar un trasplante”. De este modo podría quedar proscrita la venta de neurodatos a empresas tecnológicas, debiéndose regular específicamente las condiciones y límites para el desarrollo de las actividades que constituyan tratamiento de datos neuronales. Como se puede apreciar se catalogan los datos cerebrales como órganos del cuerpo, de forma discutible, desde nuestra consideración.

3. PROTECCIÓN DISPENSADA A LOS NEURODATOS POR EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

3.1. CONCEPTO Y NATURALEZA JURÍDICA DEL NEURODATO

En la actualidad dentro de la tipología de datos personales de carácter sensible del art. 9.1 contenida en el Reglamento de Protección de Datos no encontramos mención alguna a los neurodatos.

Con el objeto de poder dilucidar esta cuestión, citaremos el art. 1 c) del proyecto de la Ley chilena nº de Boletín 13828-19 comentado con anterioridad, el cual define los datos neuronales, de manera profusa y un tanto difusa, como “aquella información obtenida, directa o indirectamente, a través de los patrones de actividades de las neuronas, cuyo acceso está dado por neurotecnología avanzada, incluyendo sistemas de registro cerebrales tanto invasivos como no invasivos. Estos datos contienen una representación de la actividad

psíquica, tanto consciente como subconsciente, y que corresponden al más íntimo aspecto de la privacidad humana”.

En relación con este precepto destacamos la preocupación del legislador chileno por los datos neuronales provenientes del subconsciente de la persona, si bien no incluye la información que se pueda implementar en la actividad cerebral (pese al amplio concepto dado por este documento a las BCI)⁵⁰.

Del mismo modo, la *Recomendación de la OCDE sobre Innovación Responsable en Neurotecnología*, entiende, en términos muy generales, que los datos personales cerebrales son “los datos relacionados con el funcionamiento o estructura del cerebro humano de un individuo identificado o identificable que incluye información única sobre su fisiología, salud o estados mentales”⁵¹.

Ya en nuestro país, la Agencia Española de Protección de Datos define los neurodatos de forma amplia como “(...) la información que se recoge del cerebro y/o del sistema nervioso (...), incluyendo las “(...) inferencias basadas directamente en estos datos (...)”⁵². De esta manera, en nuestra opinión, no se engloba expresamente la información que pueda eventualmente incorporarse al cerebro.

Por lo que se refiere a la naturaleza del dato neurológico debemos apuntar que se trata de un dato personal, dado que pertenecen a personas identificadas o identificables⁵³. Esta información suele recogerse de personas que están identificadas, se han identificado previamente o incluso se puede sostener que identifican a una persona de manera única⁵⁴. La doctrina también aboga por calificar al neurodato como un dato personal, dado que permite identificar a la persona a la que pertenecen. Y ello resultaría así incluso en el caso de las ondas cerebrales, puesto que éstas en combinación con otras características posibilitarían la distinción de su titular⁵⁵.

Además, los neurodatos pueden quedar englobados en la categoría especial de datos, en concreto (sin perjuicio de otras opciones contenidas en el art. 9.1 del RGPD), como aquellos relativos a la salud o como datos biométricos dirigidos a identificar de manera unívoca a una persona física. Y ello con independencia de que los datos neurológicos se encuentren incluidos en un

⁵⁰ Así, un sector de la doctrina incluye en el concepto de neurodato la información que es incorporada al cerebro, véase BASTIDAS CID, Y.V.: “Neurotecnología: interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos de la Unión Europea”, *Revista Iberoamericana de Derecho Informático (Segunda Época)*, año 2, núm.11, 2021, p. 132.

⁵¹ *Recomendación sobre Innovación Responsable en Neurotecnología*, OCDE, 2019.

⁵² *EDPS TechDispatch* Agencia Española de Protección de Datos, 2024, p. 4.

⁵³ Art. 4. 1) RGPD.

⁵⁴ *EDPS TechDispatch* Agencia Española de Protección de Datos, 2024, p. 4.

⁵⁵ BASTIDAS CID, Y.V., *op. cit.*, p. 138.

historial médico, dado que los datos relativos a la salud se configurarían como un concepto más amplio que la noción “médico”⁵⁶.

Así las cosas, entendemos que resulta prioritaria la elaboración de un concepto de neurodato desde una perspectiva lo más vasta posible, con el objeto de garantizar tan información sensible, y su inclusión en el catálogo de datos personales.

En cuanto a la tipología de los neurodatos, también podemos aludir a aquellos que se refieren a la estructura del cerebro; los que muestran datos sobre la función y actividad cerebral y aquellos relacionados con el sistema nervioso periférico⁵⁷. También podemos mencionar otras clasificaciones que distinguen entre neurodatos (datos primarios), datos neuronales (registrados de forma directa o indirecta), datos mentales (representaciones mentales) y datos de neurociencia (datos derivados de mediciones)⁵⁸.

En relación con esta cuestión, debemos colegir que aquella información neuronal de la que no se pueda siquiera inferir datos personales del interesado, quedaría excluida del ámbito de aplicación de la norma.

3.2. RESPONSABILIDAD POR DAÑOS CAUSADOS POR INFRACCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LAS BCI

En términos generales, el régimen de responsabilidad contenido en el art. 82 del RGPD supone una considerable protección de la privacidad de los datos, al garantizar la indemnización de los daños y perjuicios sufridos por el titular de los datos como causa de la infracción de dicho Reglamento y que deberá satisfacer el responsable o el encargado de tratamiento.

Con carácter previo al análisis pormenorizado del citado precepto, debemos realizar unas precisiones en cuanto al régimen de responsabilidad previsto en el art. 82 del RGPD aplicable también, según nuestra consideración a los neurodatos⁵⁹.

⁵⁶ BASTIDAS CID, Y.V., *op. cit.*, p. 141.

⁵⁷ *EDPS TechDispatch* Agencia Española de Protección de Datos, 2024, pp. 5-6.

⁵⁸ *El desarrollo humanista de la neurotecnología, una nueva oportunidad para España*, Digital Future Society, 2024, nota nº 2, p. 12-13.

⁵⁹ Este precepto determina que “1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto en el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando haya incumplido con las obligaciones del presente Reglamento dirigidas específica-

La redacción ambigua del precepto que comentamos ha propiciado diversas opiniones en relación con el criterio de imputación contenido en el mismo. El legislador europeo ha prescindido de una referencia explícita a la culpa, no obstante prever una causa de exoneración en virtud de la cual quedará exento de responsabilidad el responsable o el encargado del tratamiento si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

Así, con arreglo a un sector de la doctrina, se trataría de un sistema basado en la culpa. En concreto nos encontraríamos ante una naturaleza *quasi* objetiva con inversión de la carga de la prueba de la falta de diligencia. De este modo las obligaciones del RGPD vendrían a ser estándar de diligencia a la hora de tratar los datos, con los específicos requerimientos apuntados con anterioridad en relación con los neurodatos⁶⁰.

Por otra parte, otro sector doctrinal, aboga por el carácter objetivo del sistema de responsabilidad ideado por el legislador europeo⁶¹. Si bien también se destaca, la necesidad de superación de la visión subjetiva/objetiva del sistema vigente, sobre la base de la existencia de obligaciones de medios que necesariamente obligan a valorar la diligencia del responsable o encargado⁶².

A este respecto, debemos resaltar que esta diversa tipología de deberes evoca a la distinción entre el incumplimiento de una obligación de seguridad, a la que se anuda una responsabilidad subjetiva (con inversión de la carga de la prueba) y el resto de prescripciones, a las que se vincula una responsabilidad de corte objetivo⁶³.

mente a los encargados o hay actuado al margen o en contra de las instrucciones de legales del responsable. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios (...).

⁶⁰ BUSTO LAGO, J.M.: “La responsabilidad civil y su función de tutela del derecho a la protección de datos personales: una visión desde el derecho de la Unión Europea”, *REJUR*, vol. 5, n° 10, julio/diciembre, 2022, pp. 33-35.

⁶¹ Así, RUBÍ PUIG, A.: “Daños por infracciones del derecho de protección de datos personales. El remedio indemnizatorio del art.82 RGPD”, *Revista de Derecho civil*, vol. 5, núm. 4, octubre-diciembre, 2018, p. 78 y MORENO MARTÍNEZ, J.A.: “El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el derecho interno y problemática de coexistencia con otros mecanismos protectores”, *Cuestiones clásicas y actuales del Derecho de daños: Estudio en homenaje al profesor D. Roca Guillamón*, (coord. J. Ataz López, J.A. Cobacho Gómez; J. Roca Guillamón (hom.), A. Díaz-Bautista (aut.), vol. 3, Aranzadi, Pamplona, 2021, p. 38.

⁶² SANTOS MORÓN, M.J.: “La responsabilidad por incumplimiento de la normativa de datos personales (art. 82 RGPD)”, p. 246, disponible en <https://nomos-elibrary.de>, 2023, consultado el 28.8.2024 y en el mismo sentido RUBÍ PUIG, A., *op. cit.*, pp. 63-64.

⁶³ Tipología analizada por BUSTO LAGO, J.M., *op. cit.*, p. 31.

En nuestra opinión, y con mayor motivo respecto del tratamiento de los neurodatos, debiera optarse por interpretar el precepto desde una perspectiva objetiva, no obstante, la confusa dicción del artículo objeto de estudio. Y ello al abrigo de diversos y sustanciales motivos: los graves riesgos inherentes a los derechos más fundamentales de la persona; la especial vulnerabilidad de los grupos a los que se dirigen estas tecnologías (personas menores, enfermos, trabajadores, consumidores, personas mayores, etc.); la extrema sensibilidad de la información a tratar; la gravedad y en ocasiones irreversibilidad de los daños individuales o colectivos; el elevado número de titulares susceptibles de ser afectados; la incertidumbre acerca de las consecuencias sobre la salud de los usuarios de las neurotecnologías; el beneficio económico; los variados problemas de la aplicación de algoritmos; el estricto deber de garantía que implica el principio de responsabilidad proactiva; la expresión “en modo alguno” del art. 82.3 del RGPD y las dificultades probatorias de los daños de unas tecnologías basadas en la inteligencia artificial.

En sede judicial, el TJUE ha tratado recientemente esta cuestión determinando expresamente que nos encontramos ante un sistema de responsabilidad basado en la culpa. Textualmente, la STJUE (Sala Tercera), de 21 de diciembre de 2023, indica que “(...) del análisis conjunto de estas diferentes disposiciones del art. 82 del RGPD se desprende que este artículo establece un régimen de responsabilidad por culpa en el que la carga de la prueba no recae sobre la persona que ha sufrido los daños y perjuicios, sino sobre la responsabilidad del tratamiento (...)”, dado que un “(...) Por otra parte, un régimen de responsabilidad objetiva no garantizaría la consecución del objetivo de seguridad jurídica perseguido por el legislador (...)”⁶⁴.

Otro punto de interés en relación con el art. 82 del RGPD que examinamos, haría referencia a la determinación de la naturaleza contractual o extracontractual de esta responsabilidad. Entendemos que en función del tipo de relación entre el titular de los neurodatos y el responsable/encargado del tratamiento, nos hallaremos ante uno u otro supuesto⁶⁵. Si bien es cierto que los supuestos de responsabilidad extracontractual serán los más habituales⁶⁶.

Finalmente, otra cuestión que se suscita con carácter general se refiere a la compatibilidad, la cual secundamos, de la acción de responsabilidad que ahora comentamos con otros mecanismos tuitivos, como puede ser la responsabilidad aquiliana contenida en el art. 1902 del CC, la responsabilidad contractual 1101, o las acciones protección honor establecidas en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad perso-

⁶⁴ (JUR/2023/449592)

⁶⁵ BUSTO LAGO, J.M., *op. cit.*, p. 30.

⁶⁶ MORENO MARTÍNEZ, J.A., *op. cit.*, p. 22.

nal y familiar y a la propia imagen⁶⁷. Todo ello sin perjuicio de la denuncia de las infracciones ante la Autoridad de control vía art. 72 del RGPD, la cual se configura de manera independiente.

3.2.1. Sujetos

En relación con la legitimación activa para la interposición de la presente acción indemnizatoria, la misma corresponde a la persona física, excluyéndose con ello a las personas jurídicas. Sobre este particular consideramos que debió haberse adoptado el término titular de los datos personales o interesado, entendido como toda persona física identificada o identificable⁶⁸.

Por tanto, las personas jurídicas quedarían excluidas de dicha protección, cuestión obvia en el caso de los neurodatos. Igualmente, carecerían de dicho amparo las personas fallecidas, pudiendo reclamar en estos supuestos aquellos legitimados con arreglo a la LO 1/1982, de 5 de mayo, dado que el registro de la información sobre la actividad cerebral, al permitir evidenciar rasgos sobre la personalidad, patologías, tendencias, etc., bien pudiera propiciar daños contra el honor de la persona fallecida⁶⁹.

Legitimados pasivamente, además de la persona física, se encuentran las personas jurídicas y las Administraciones Públicas, dado que son susceptibles de erigirse en responsables o encargados del tratamiento de neurodatos. Piénsese a tal efecto en las posibles aplicaciones de la Neurotecnología en la Administración de Justicia, Educativa o los tratamientos médicos o rehabilitadores dispensados para tratar las muy diversas patologías neuronales que hemos analizado con anterioridad, por no mencionar la actividad investigadora desplegada en estos sectores⁷⁰.

Relacionado con esta cuestión, debemos indicar que un sector de la doctrina que defiende la aplicación de la normativa sustantiva sobre responsabilidad patrimonial de la Administración Pública⁷¹.

⁶⁷ Defiende la compatibilidad de la acción objeto del presente estudio y de la acción de la LO 1/1982 MORENO MARTÍNEZ, J.A., *op. cit.*, p. 521.

⁶⁸ Véase respectivamente BUSTO LAGO, J.M., *op. cit.*, p. 8 y MORENO MARTÍNEZ, J.A., *op. cit.*, p. 523-524.

⁶⁹ Aplicando la argumentación expuesta por BUSTO LAGO, J.M., *op. cit.*, pp. 7-8.

⁷⁰ De acuerdo con el art. 4.7 del RGPD, es toda persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Debemos añadir que también pueden existir sujetos afectados de forma indirecta, RUBÍ PUIG, A., *op. cit.*, pp. 60-61.

⁷¹ Así PLAZA PENEDÉS, J.: "Protección de datos e indemnización por daños en la reciente jurisprudencia del TJUE", *Daño y resarcimiento*, Sepin, Madrid, 2024, pp. 397-425, p. 422 y MORENO MARTÍNEZ, J.A., *op. cit.*, pp. 520-521.

No obstante, en el supuesto de entes públicos, el procedimiento se sustanciaría ante la jurisdicción contencioso-administrativa, dado que el art. 82.6 del RGPD remite a las legislaciones nacionales para determinar el órgano judicial competente ante quien plantear la acción de responsabilidad⁷².

Además, el propugnar que la responsabilidad de los sujetos que traten neurodatos ostenta un carácter objetivo, resultaría coherente con el título de imputación previsto en el art. 106.2 de la CE regulador de la responsabilidad patrimonial de las Administraciones Públicas⁷³.

3.2.2. Requisitos exigidos

Las exigencias requeridas para la apreciación de dicha responsabilidad son, como resulta consabido, una infracción legal, daño y nexo causal entre ambos elementos.

A) Infracción

Por lo que respecta a la trasgresión de la normativa de protección de datos contenida en el RGPD, debemos apuntar que como resultado obvio, en materia de BCI se han de respetar con más celo, si cabe, los deberes establecidos para el tratamiento por el RGPD⁷⁴. Centrándonos en la figura del responsable del tratamiento, como eje de todo el sistema de responsabilidad, debemos indicar que el mismo debe asegurarse de respetar: los principios de licitud; lealtad; transparencia; limitación de la finalidad; minimización; exactitud; plazo de conservación; integridad; confidencialidad; los derechos de los interesados y adoptar las medidas de seguridad adecuadas frente al riesgo que genere el tratamiento en cuestión⁷⁵.

Así las cosas, la AEPD ha analizado los axiomas en los que se debe incidir especialmente a la hora de efectuar el tratamiento de neurodatos. Así, el principio de proporcionalidad y minimización, implican la recogida de los

⁷² En este sentido SANTOS MORÓN, M.J., *op. cit.*, p. 23 y BUSTO LAGO, J.M., *op. cit.*, p. 25.

⁷³ Además del responsable del tratamiento y del encargado, la doctrina también incluye a otros sujetos como eventuales responsables subencargados, delegados de protección de datos o representantes de los responsables o encargados, quienes en la medida en que intervengan en el tratamiento de neurodatos podrán estar legitimados pasivamente, así, BUSTO LAGO, J.M., *op. cit.*, p. 14-25; MORENO MARTÍNEZ, J.A., *op. cit.*, pp. 528-532 y RUBÍ PUIG, A., *op. cit.*, pp. 70-73.

⁷⁴ Añade también el respeto a actos delegados y de ejecución del RGPD y contrarios a las legislaciones de desarrollo de los Estados de la Unión, MORENO MARTÍNEZ, J.A., *op. cit.*, pp. 537; BUSTO LAGO, J.M., *op. cit.*, p. 27 y RUBÍ PUIG, A., *op. cit.*, p. 58.

⁷⁵ SANTOS MORÓN, M.J., *op. cit.*, p. 238-239.

datos adecuados, pertinentes y limitados a los fines del tratamiento. Esta idea contrasta con la ingente cantidad de datos que pueden recolectar las BCI por lo que deberá ajustarse su uso a este principio. En segundo lugar, el respeto a la exactitud de los datos colisiona con la plasticidad cerebral, debida a la cual los neurodatos son cambiantes, debiéndose por tanto efectuar las pertinentes actualizaciones. Por su parte, el principio de transparencia, supone que el interesado, no obstante, la complejidad del funcionamiento de las BCI deberá entender las consecuencias del tratamiento y sus potenciales implicaciones. Finalmente, la lealtad debe ser entendida como la evitación de efectos adversos injustificados, como son las discriminaciones que pueden presentarse por los sesgos algorítmicos⁷⁶.

También en relación con la inobservancia del RGPD, debemos destacar la crucial problemática que suscita el consentimiento como base legitimadora del tratamiento de neurodatos⁷⁷.

No obstante, la tutela legal establecida para esta categoría especial de datos, las prácticas empresariales conculcan en ocasiones los requisitos establecidos para que el consentimiento sea base suficiente para el tratamiento de los neurodatos.

En este sentido, destacaremos el estudio de la Fundación Neurorights (Titulado finalmente como *Safeguarding Brain Data: Assessing the Privacy Practices of Consumern Neurotechnology Companies*). Este informe, examina las prácticas de un nutrido número de empresas muy influyentes en el sector neurotecnológico, alcanzando, como veremos conclusiones bastante desoladoras. A este respecto debemos señalar, en primer lugar, que los dispositivos basados en Neurotecnología sobre los que se despliega esta investigación son productos destinados al bienestar, entretenimiento y también a la investigación ofertados a los consumidores.

De este modo, el documento analiza cinco áreas especialmente comprometidas. A saber, en primer lugar, el acceso a la información, centrándose en este punto el estudio en el acceso a los documentos de políticas, la posibilidad de contactar con la empresa y la notificación de cambios de política sobre privacidad. En segundo lugar, en cuanto a la recopilación y almacenamiento de datos, se examina los tipos de datos recopilados, la cantidad, la retención y la limitación del almacenamiento. En tercer lugar, en relación con el intercambio de datos, encontramos el modo de compartir datos con terceros, el

⁷⁶ EDPS TechDispatch Agencia Española de Protección de Datos, 2024, pp. 16-19.

⁷⁷ Resalta la problemática de la regulación de los límites del consentimiento en el ámbito de las neurotecnologías Reche Tello, N.: *Mens iura fundamentalia: La neurotecnología ante la Constitución*, Cuaderno núm. 2, Cuadernos de la Cátedra de Relaciones Privadas Internacionales de la UMH-ICAO, Colex, A Coruña, 2024, pp. 258-260.

intercambio de datos con organismos oficiales y la venta de datos a terceros. En cuarto lugar, por lo que respecta a los derechos del usuario, el citado estudio explora las prácticas empresariales en relación con la retirada del consentimiento y la eliminación de los datos. Y finalmente, el apartado de seguridad de datos y protección aborda la anonimización y pseudonimización, el cifrado y la notificación de violaciones de seguridad.

De entre la ingente cantidad de datos que incluye el informe, traeremos a colación algunos de ellos a los fines del presente estudio sobre el consentimiento de los consumidores al tratamiento de los neurodatos por parte de las empresas en cuestión. De este modo, en relación con el acceso a la información, más del 26% de las empresas no tienen política de privacidad disponible y sólo el 33% se compromete a notificar al consumidor los cambios en la política de protección de datos. Por lo que respecta a la recopilación de datos y almacenamiento, más del 96% de las empresas tienen acceso a los datos neuronales de los consumidores sin limitaciones significativas. En cuanto al controvertido tema relativo a la capacidad de compartir datos con terceros, se llega a la conclusión de que más del 96% de las empresas pueden transferir los datos. En el apartado de derechos de los usuarios, tan solo el 53% de las empresas mencionan el derecho a retirar el consentimiento al tratamiento de datos y únicamente el 46% de las organizaciones otorgan el derecho a eliminar los datos de los consumidores. Finalmente, en materia de protección, el 57% de las empresas mencionan la fórmula de anonimización, sólo el 20% menciona el cifrado de datos y sólo el 16% se compromete a notificar las brechas de seguridad. Como conclusión, se colige que el 90% de las empresas no poseen medidas adecuadas para proteger los neurodatos⁷⁸. Esta mala *praxis* empresarial difícilmente colma las exigencias contenidas en el RGPD en relación con la prestación válida del consentimiento como base jurídica del tratamiento de datos y el respeto de los derechos de los interesados. De esa manera la causación de daños debida a la inobservancia de las referidas exigencias generaría la correspondiente responsabilidad civil al amparo del art. 82 del RGPD.

Cuestiones entorno a los requisitos del consentimiento en el ámbito del tratamiento de neurodatos, si bien sin exigencia de responsabilidad civil por daños, ya se han planteado en la jurisdicción chilena. Así, nos referiremos a la Sentencia de la Corte Suprema de Chile, de 9 de agosto de 2023⁷⁹. Resulta interesante resaltar en este caso el hecho de que demandate, un senador chile-

⁷⁸ GENSER J. Y YUSTE, R.: *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*, Neurorights Foundation, Nueva York, 2024 y BERBELL, C.: “La Neurorights Foundation advierte sobre los peligros ocultos de la neurotecnología en un novedoso informe”, abril, 2024, disponible en <https://confilegal.com>, revisado el 25.8.2024.

⁷⁹ Sentencia de la Corte Suprema de Chile, de 9 de agosto de 2023, Rol 105.065-2023, disponible en <https://www.pjud.cl>, consultada el 9.9.2024.

no defensor de ellos neuroderechos adquirió una diadema neurotecnológica destinada a registrar la actividad cerebral, con la posibilidad de cargar los datos en la plataforma para poder visualizarlos. El demandante comprobó, entre otros extremos, la imposibilidad de acceso a sus datos, de no efectuar un pago previo. Así las cosas, el Alto Tribunal decretó que la empresa demandada violentaba el derecho a la privacidad, integridad física y mental del demandante.

Al hilo de la problemática del consentimiento, debemos analizar el documento de la AEPD sobre adecuación del RGPD a la Inteligencia Artificial, en el que se incide en la idea de proporcionar al interesado sometido a decisiones automatizadas o elaboración de perfiles de la información significativa sobre la lógica aplicada y sobre consecuencias previstas, de acuerdo con el art. 13.2.f) del RGPD, de manera que se entienda el funcionamiento del algoritmo. Así sería oportuno hacer referencia a los neurodatos empleados y su importancia para la toma de la decisión; la calidad de los mismos; perfiles e implicaciones; existencia de supervisión humana, etc.⁸⁰.

También debemos traer a colación en este apartado, el análisis del riesgo, como reflejo del principio de responsabilidad proactiva y cuya infracción sería susceptible de generar la correspondiente responsabilidad civil.

En este sentido cabe destacar que las BCI bien pueden quedar subsumidas en cualquiera de los supuestos de riesgo del art. 75 del RGPD. Finalmente, entendemos preceptiva la elaboración de la Evaluación de Impacto de la Privacidad de Protección de Datos (EIPD), dado que el tratamiento de neurodatos mediante las interfaces objeto de estudio pueden ser considerado como eventuales generadoras alto riesgo, tal y como se desprende de los nueve criterios establecidos a este fin por el “Grupo Protección de Datos” del art. 29. De esta manera se incluyen en esta categoría los sistemas de evaluación o puntuación; toma de decisiones automatizadas con efecto jurídico significativo; observación sistemática; datos sensibles; tratamiento de datos a gran escala; asociación de conjuntos de datos; datos pertenecientes a interesados vulnerables; uso innovador de nuevas soluciones tecnológicas, etc.⁸¹.

Por tanto, se deberán adoptar las medidas concretas y adecuadas para la gestión del riesgo, tales como minimizar los neurodatos recopilados; agregarlos; ocultarlos para limitar su exposición; separar los contextos de tratamiento; mejorar la información a los interesados; proporcionar medidas de

⁸⁰ *Adecuación al RGPD de tratamientos que incorporen Inteligencia Artificial. Una introducción*, Agencia Española de Protección de Datos, 2020, p. 24.

⁸¹ *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, del 4.4.2017*. Establece la obligación de la evaluación de impacto al tratar neurodatos mediante BCI, BASTIDAS CID, Y.V., *op. cit.*, 160.

control; cumplir y demostrar el cumplimiento de la normativa de protección del tratamiento de neurodatos, etc. También en relación con los registros de datos neuronales resultará conveniente determinar los sujetos con acceso a la información y proporcionar la trazabilidad de los neurodatos entre todos los sujetos intervinientes⁸².

En relación con el cumplimiento de las medidas de seguridad adecuadas del art. 24 RGPD, podría también postularse la aplicación del encriptamiento de documentos y carpetas que contengan neurodatos o incluso la utilización de la tecnología *blockchain*, si bien en podrían plantearse dudas en relación con los derechos de rectificación o supresión del interesado⁸³.

B) Daño

De acuerdo con la dicción legal, el menoscabo sufrido puede presentar naturaleza material o inmaterial. Esta previsión la debemos conectar con el Considerando 146 del RGPD, el cual propugna una indemnización total y efectiva de por los daños y perjuicios padecidos y con el extenso catálogo de daños contenido en el Considerando 85, en el que expresamente se alude, entre otros, también a los de carácter físico⁸⁴.

Del mismo modo, el STJUE, parte de un concepto amplio de daño. Así la STJUE (Sala Tercera), de 4 de mayo de 2023, en el asunto C-300/21 ha establecido que «(...) una indemnización pecuniaria basada en esta disposición de be considerarse “total y efectiva” si permite compensar íntegramente los concretos daños y perjuicios sufridos (...)»⁸⁵.

De este modo podemos postular que los daños contra la vida, físicos, psicológicos, morales, etc. quedarían incluidos en el precepto, los cuales son susceptibles de ser provocados sin lugar a dudas por las nuevas neurotecnologías.

Como resulta consabido los daños materiales presentan mayores facilidades en cuanto a la determinación de su existencia y extensión, a diferencia de los perjuicios inmateriales, si bien pueden existir supuestos de especial complejidad. Sobre este particular, se presentan especialmente interesantes los casos de pérdida de oportunidad, los cuales tendrían cabida como daño indem-

⁸² Sobre la base de las medidas específicas determinadas por la AEPD para la gestión del riesgo expuestas en la *Adecuación al RGPD de tratamientos que incorporen Inteligencia Artificial. Una introducción*, Agencia Española de Protección de Datos, 2020, p. 32, 39 y 43.

⁸³ Sobre la utilización de las técnicas de encriptamiento para minimizar los riesgos de ciberataques véase PLAZA PENEDÉS, J., *op. cit.*, pp. 424.

⁸⁴ Propugna un concepto amplio de daño RUBÍ PUIG, A., *op. cit.*, pp. 74-75 y PLAZA PENEDÉS, J., *op. cit.*, p. 404.

⁸⁵ (STCE 2023/79)

nizable, en relación verbigracia, con los sesgos algorítmicos y la inequidad de acceso a las neurotecnologías.

Por otra parte, la redacción legal también permite dar cabida a los daños morales, los cuales pueden llevar aparejados daños patrimoniales⁸⁶.

Un sector de la doctrina aprecia la existencia de este tipo de daños, en los supuestos de infracciones de la normativa de protección de datos, pero en los que no se haya materializado ningún daño, sobre la base de configurar el derecho a la protección de datos como el derecho de la persona a controlar los datos de su titularidad⁸⁷.

Sobre la base en este argumento, con mayor motivo, los supuestos que se puedan originar de mejoramiento mental no consentido o de manipulación de la identidad o de la conducta por infracción del derecho a la protección de datos, deben incluirse en el concepto de daño moral, sin perjuicio de que estemos incluso también ante daños psicológicos o incluso personales o patrimoniales, de ser constatados.

Un supuesto concreto de daño moral se puede apreciar en relación con el temor experimentado a que sean utilizados los propios datos, el cual se acrecienta sin lugar a dudas en el caso de los neurodatos. Esta cuestión ha sido analizada recientemente por el Tribunal de Justicia de la Unión Europea en la Sentencia de 14 de diciembre de 2023, asunto C-340/21, al exigir que el interesado demuestre la causación de daños inmateriales y añadir que el temor padecido ha de ser fundado, teniendo en cuenta las circunstancias específicas del caso y del interesado. Sobre este punto, debemos señalar que la doctrina incide en la necesidad de la cuantificación razonada y razonable del daño moral⁸⁸.

Por último, apuntar que, la STJUE (Sala Tercera), de 4 de mayo de 2023, ha destacado la innecesariedad de una cuantía mínima del daño para la apreciación de responsabilidad⁸⁹.

C) Relación causal

En relación con el nexo causal, el RGPD no contiene ninguna previsión. Las dificultades probatorias en materia de neuroderechos son complejas en

⁸⁶ BUSTO LAGO, J.M., *op. cit.*, p. 42 y SANTOS MORÓN, M.J., *op. cit.*, p. 248.

⁸⁷ SANTOS MORÓN, M.J., *op. cit.*, p. 249.

⁸⁸ (JUR 2023/440264). Sobre esta cuestión véase PLAZA PENEDÉS, J.: “La responsabilidad civil del artículo 82 RGPD en brechas seguridad”, *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 4, 2024, pp. 5-6.

⁸⁹ (STCE 2023/79)

relación, por ejemplo, con la actividad de los algoritmos utilizados, la acreditación del cumplimiento de las complejas medidas de seguridad adecuadas sobre el tratamiento de neurodatos o incluso el concreto destino dado a esta información a través de la Red.

Partiendo de una concepción objetiva del sistema legal, tan solo cabría imputar responsabilidad al responsable del tratamiento o encargado en el tradicional supuesto de fuerza mayor, englobando ésta todos aquellos hechos extraños al desarrollo de su actividad de tratamiento de neurodatos desplegada. En términos más precisos, la *vis maior* quedaría circunscrita a los hechos atípicos a la actividad de tratamiento de datos neuronales⁹⁰. También tendrían fuerza exoneradora para la doctrina los supuestos de culpa exclusiva de la víctima o hecho de un tercero⁹¹.

Sobre esta cuestión debemos indicar que los supuestos de brecha de seguridad de neurodatos, desde una perspectiva objetiva, podrían quedar circunscritos al ámbito de actuación del responsable o encargado del tratamiento de los mismos, dado que son riesgos típicos de la actividad, debiéndose considerar, en consecuencia, como caso fortuito generador de responsabilidad.

La doctrina partidaria de una concepción subjetiva del título de imputación contenido en la norma objeto de estudio, resalta que el hecho de tomar medidas frente a las violaciones de seguridad (protocolos de buenas prácticas/instrumentos de certificación), si bien minora el riesgo, no es el único elemento a tomar en consideración, dado que puede haberse infringido otros deberes, como el de notificación de la brecha de seguridad, generándose, por tanto, responsabilidad⁹².

De optarse por una interpretación basada en la culpa del régimen de responsabilidad que comentamos, la exoneración del responsable o del encargado se produciría si éstos probasen que el hecho no les es imputable “en modo alguno”. Esta expresión nos indica que deberá acreditarse un cumplimiento muy elevado de los deberes establecidos en el RGPD, establecidos como estándar de diligencia, en consonancia con el concepto de responsabilidad activa.

En relación con este tema el Alto Tribunal, mediante STJUE (Sala Tercera), de 14 de diciembre de 2023, ha decretado que el hecho de padecer un ciberataque no implica responsabilidad *iuris et de iure* por no cumplir con las medidas de seguridad. Y que, del mismo modo, tampoco cabe exone-

⁹⁰ MEDINA CRESPO, M./MEDINA ALCOZ, M. Y MEDINA ALCOZ, L.: «La fuerza mayor y su condicionada virtualidad exoneradora en sede de responsabilidad civil», p. 9-10, disponible en <https://www.asociacionabogadosrcs.org>, consultado el 15.9.2024.

⁹¹ MORENO MARTÍNEZ, J.A., *op. cit.*, p. 538.

⁹² Sobre esta cuestión véase BUSTO LAGO, J.M., *op. cit.*, p. 28.

ración, sin prueba en contrario, por haber aplicado medidas de seguridad. Debiéndose, por tanto, analizar si se han adoptados las mínimas medidas de seguridad para prevenir el ciberataque⁹³.

BIBLIOGRAFÍA

- ALONSO-VALERDI, L.M./Arteola, M.A. y ARGÜELLO GARCÍA J.: “Interfases cerebro-computadora: conceptualización, retos de diseño e impacto social”, *Revista Mexicana de Bioingeniería Mecánica*, vol. 40, núm. 3, septiembre-diciembre, 2019, pp. 1-18.
- ARAYA-PIZARRO, SEBASTIÁN C. Y ESPINOZA PASTÉN, L.: “Aportes desde las neurociencias para la comprensión de los procesos de aprendizaje en los contextos educativos”, *Propósitos y representaciones*, 2020, vol. 8, núm. 1, e312, pp. 1-10.
- ARMENGOL-URPI, A./KOVACS, R. Y SARMA, S.E.: “Brain-Hack: Remotely Injecting False Brain-Waves with RF to take control of Brain Computer Interfaces”, *CPSIoTSec´23*, noviembre, 26, 2023 pp. 53-66.
- BAJATIERRA RUÍZ, M.: “Una argumentación moral de los neuroderechos humanos”, *Revista Electrónica de Estudios Penales y de la Seguridad*, núm. 12, 2023, pp. 1-26.
- BASTIDAS CID, Y.V.: “Neurotecnología: interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos de la Unión Europea”, *Revista Iberoamericana de Derecho Informático (Segunda Época)*, año 2, núm.11, 2021, pp. 101-176.
- BERBELL, C.: “La Neurorights Foundation advierte sobre los peligros ocultos de la neurotecnología en un novedoso informe”, abril, *Conflegal*, 2024, disponible en <https://conflegal.com>, revisado el 25.8.2024.
- BUSTO LAGO, J.M.: “La responsabilidad civil y su función de tutela del derecho a la protección de datos personales: una visión desde el derecho de la Unión Europea”, *REJUR*, vol. 5, n° 10, julio/diciembre, 2022, pp. 1-60.
- CORREDOR, K. Y CÁRDENAS, F.P.: «“Neuro-lo que sea”: inicio y auge de una neurociencia para el siglo XXI», *Revista Iberoamericana de Psicología*, vol. 49, núm. 1-3, 2017, pp. 89-90.
- DE ASÍS, R.: “Sobre la propuesta de los neuroderechos”, *Derechos y libertades*, núm. 47, Época II, junio 2022, pp. 51-70.
- DE LEÓN BARRIOS, V.H.: *Neurotecnología: el futuro*, Universidad de San Carlos de Guatemala, 2022.
- ESCOBAR VIDARTE, O.A./OROZCO MERA, J. Y ORDÓÑEZ CASTILLO, J.A.: “Precisión en implantación de electrodos para estimulación cerebral profunda para el mane-

⁹³ (JUR 2023/440264). Analizada en el tema que nos ocupa por PLAZA PENEDÉS, J., *op. cit.*, pp. 5-6.

- jo de trastornos del movimiento”, *Revista EIA*, año IX, vol. 19, edición núm. 37, enero-junio, 2022, p.p. 1-15.
- GARCÍA, L.V. Y WINICKOFF, D.E.: “Brain-computer interfaces and governance system: Upstream approaches”, *OECD Science, Technology and Industry Working Papers*, núm. 1, 2001., pp. 1-41.
- GARCÍA HERRERO, C.A.: “Análisis de los algoritmos para la caracterización de señales cerebrales EGG”, Ingeniería electrónica, *Ingeniería electrónica*, Universidad Cooperativa de Colombia, Bogotá, 2021.
- GENSER J. Y YUSTE, R.: *Safeguarding Brain Data: Assessing the Privacy Practices of Consumern Neurotechnology Companies*, Neurorights Foundation, Nueva York, 2024.
- IENCA, M. Y ANDORNO, R.: “Hacia nuevos derechos humanos en la era de la neurociencia y neurotecnología”, *Análisis Filosófico*, núm. 41, vol. 1, mayo 2021, pp. 141-185.
- MARZUCA ABUMOHOR, T.R.: *Neuroderecho: Análisis de la ley N° 21.383 (Boletín N° 13.827) y el Boletín N° 13.828 sobre neuroprotección e indemnidad mental*, Universidad de Chile, Santiago, 2023, disponible en <https://repositorio.uchile.cl>, consultado el 22.8.2024.
- MAISELI B./ABDALLA, A.T./MASSAWE, L.V./MERCY MBISE/MKOCHA, K./NASSOR NASSOR, A./ISMAIL, M./MICHAEL, J. Y KIMAMBO, S.: “Brain-computer interface: tred, challenges and theats”, *Brain Informatics*, 10, 20, 2023, pp. 1-16.
- MEDINA CRESPO, M./MEDINA ALCOZ, M Y MEDINA ALCOZ, L.: “La fuerza mayor y su condicionada virtualidad exoneradora en sede de responsabilidad civil”, p. 1-16, disponible en <https://www.asociacionabogadosrcs.org>, consultado el 15.9.2024.
- MONASTERIO ASTOBIZA, A./ AUSÍN, T./TOBOSO, M./MORTE FERRER, APARICIO PAYÁ, R, Y LÓPEZ, D.: “Traducir el pensamiento en acción: Interfaces cerebro-máquina y el problema ético de la agencia”, *Revista de Bioética y Derecho*, núm. 46, 2019, pp. 29-49.
- MORENO MARTÍNEZ, J.A.: “El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el derecho interno y problemática de coexistencia con otros mecanismos protectores”, *Cuestiones clásicas y actuales del Derecho de daños: Estudio en homenaje al profesor D. Roca Guillamón*, (coord. J. ATAZ LÓPEZ, J.A. COBACHO GÓMEZ: J. ROCA GUILLAMÓN (hom.), A. DÍAZ-BAUTISTA (aut.), vol. 3, Aranzadi, Pamplona, 2021, pp. 515-567.
- NARVAEZ MORA, M.: “Neuroderecho: el sentido de la acción no está en el cerebro”, *Revista de Teoría del Derecho de la Universidad de Palermo*, años 1, núm. 2, noviembre, 2014, pp. 125-148.
- PLAZA PENEDÉS, J.:
- “La responsabilidad civil del artículo 82 RGPD en brechas seguridad”, *Revista Aranzadi de Derecho y nuevas tecnologías*, N.º 4, 2024, pp. 1-7.

- “Protección de datos e indemnización por daños en la reciente jurisprudencia del TJUE”, *Daño y resarcimiento*, Sepin, Madrid, 2024, pp. 397-425.
- REGUERA ANDRÉS, M.C. Y CAYÓN DE LAS CUEVAS, J.: “La garantía de los neuroderechos: a propósito de las iniciativas emprendidas para su reconocimiento”, *Derecho y Salud*, vol. 31 (extraordinario), pp. 212-221.
- RECHE TELLO, N.: *Mens iura fundamentalia: La neurotecnología ante la Constitución*, Cuaderno núm. 2, Cuadernos de la Cátedra de Relaciones Privadas Internacionales de la UMH-ICAO, Colex, A Coruña, 2024.
- RESTREPO, J.E.: “Los límites epistemológicos de las neurociencias: la falacia de la neurolo que sea”, *Revista de Psicología Universidad de Antioquía*, vol. 11 (2), 2019, pp. 201-224.
- RUBÍ PUIG, A.: “Daños por infracciones del derecho de protección de datos personales. El remedio indemnizatorio del art.82 RGPD”, *Revista de Derecho civil*, vol. 5, núm. 4, octubre-diciembre, 2018, pp. 53-87.
- RUÍZ MARTÍNEZ, J.: “Neurólogos españoles ponen en duda el anuncio de Elon Musk: No es una publicación científica”, <https://cadenaser.com>, revisado el 25.7.2024.
- SANZ DE GALDEANO, M.: “La Declaración de León sobre la neurotecnología europea: Un primer paso necesario”, *Diario la Ley*, Sección Ciberderecho, núm. 77, noviembre, 2023, disponible en <http://diariolaley.laleynext.es>, consultado el 22.8.2024.
- SANTOS MORÓN, M.J.: “La responsabilidad por incumplimiento de la normativa de datos personales (art. 82 RGPD)”, pp. 229-251, disponible en <https://nomos-library.de>, 2023, consultado el 28.8.2024.
- SCHERMER, M.: “Ethical issues in Deep brain stimulation”, *Frontiers in integrative neuroscience*, mayo, vol. 5, art. 17, 2011, pp. 1-5.
- VARGAS MENDOZA, M.I./MANRIQUE MOLINA, F.E.R. Y YÁÑEZ NÚÑEZ, L.: “Neurociencia y Derechos Humanos: rama del bioderecho para fundamentar el derecho”, *Bioderecho.es*, núm. 15, enero-junio, Centro de Estudios en Bioderecho, ética y Salud, Universidad de Murcia, 2022, pp. 1-21.
- XIAO-YU Y BIN YE: “The functional differentiation of brain computer interfaces (BCIs) and its ethical implications”, *Humanities & Social Sciences Communications*, 2023, pp. 1-9.
- XIAYING ZHANG/ZIYUE MA/HUAIJIN ZHENG/TONGKENG LI/KEXIN CHEN/XUN WANG/CHENTING LIU/LINXI XU/XIAOHANG WU/DUORU LIN Y HAOTIAN LIN: “The combination of brain-computer interfaces and artificial intelligence: applications and challenges”, *Annals of Transnational Medicine*, jun, 8 (11): 712, pp. 1-17.
- YUSTE, R.: *Las nuevas neurotecnologías y su impacto en la ciencia, medicina y sociedad*, Lecciones Cajal, Universidad de Zaragoza, 2019, disponible en <https://puz.unizar.es>, consultado el 29.8.2024.

- YUSTE, R./GENSER, J. Y HERRMANN, S.: “It’s time for neurorights”, *Horizons*, núm. 18, 2021, pp. 154-164.
- YUSTE, R./GOERING, S./AGÜERA Y ARCAS, B./GUOQUIANG BI/ CARMENA, J.M./ CARTER, A./FINS, J.J./FRIESEN, P./GALANTE, J./HUGGINGS, J.E./ILLES, J./ KELLMAYER, P./KLEIN, E./MARBLESTONE, A./MITCHELL, C./PARENS, E./ PHAM, M./RUBEL, A./NORHIRO SEDATO/SPECKER SULLIVAN, L./TEICHER, M./ WASSERMAN, D./WEXLER, A./WHITTAKER, M. Y WOLPAW, J.: “Four ethical priorities for neurotechnologies and IA”, *Nature*, vol. 551, 2017, pp. 159-163.

Encaje del sistema de Inteligencia Artificial utilizado con determinados fines médicos en algunas de las cuestiones suscitadas al amparo del régimen de responsabilidad por productos defectuosos¹

MARÍA JORQUI AZOFRA

*Profesora de Derecho Civil.
Universidad Pública de Navarra*

Sumario: 1. INTRODUCCIÓN; 2. EL SISTEMA DE IA COMO PRODUCTO; 3. EL SISTEMA DE IA COMO PRODUCTO SANITARIO; 4. ¿QUÉ DETERMINA EL CARÁCTER DEFECTUOSO DEL SISTEMA DE IA?; 5. SISTEMA DE EXHIBICIÓN DE PRUEBAS Y CARGA DE LA PRUEBA; 6. CAUSAS DE EXONERACIÓN: ESPECIAL CONSIDERACIÓN A LOS RIESGOS DEL DESARROLLO; 7. CONCLUSIONES.

1. INTRODUCCIÓN

La actual Directiva del Consejo de 25 de julio de 1985 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, (Directiva 85/374/CEE), debía revisarse a la luz de los

¹ El presente trabajo es parte del proyecto de Investigación “Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos” (TED2021-129472B-00/MICINN “Next Generation EU” /PRTR) y del proyecto PID2022-136964NB-I00 El Derecho ante la Salud Digital, Personalizada y Robótica (SALUDPYR) financiado por MCIN/ AEI /10.13039/501100011033/ y por FEDER Una manera de hacer Europa, así como del proyecto de investigación “Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos” (TED2021-129472B-00/MICIN.

avances de las nuevas tecnologías, incluida la inteligencia artificial (IA), para adaptar algunos de sus conceptos a estas. Se pretende garantizar, entre otros objetivos, que las personas perjudicadas puedan disfrutar del mismo nivel de protección con independencia de la tecnología de que se trate.

En este trabajo examinaremos algunas cuestiones que podrían plantearse cuando el producto es un sistema de IA que es utilizado para la toma de decisiones clínicas; en particular, un sistema de IA que es usado para el diagnóstico basado en imagen médica. Analizaremos esto a la luz de cómo han quedado establecidos determinados asuntos y conceptos en la reciente Resolución Legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, (RLPEPDRPD)².

La adopción de sistemas de IA en el ámbito sanitario está transformando el panorama de la prestación de los servicios de salud. La IA tiene múltiples aplicaciones en este contexto, tanto en la investigación científica como en la asistencia sanitaria. Se utiliza, por ejemplo, para los siguientes fines: la interpretación diagnóstica de imágenes en diversas especialidades (radiología, dermatología, oftalmología, anatomía patológica, oncología, etc.)³; la interpretación de electrocardiogramas⁴; el análisis de grandes volúmenes de información (derivada de las ciencias ómicas, datos clínicos, imágenes, etc.), el hallazgo de patrones que permiten mejorar la prevención y predicción de riesgos de enfermedad, la detección y diagnóstico temprano, y la monitorización y tratamiento de enfermedades (favoreciendo el progreso de la medicina personalizada)⁵; la cirugía

² P9_TA(2024)0132. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM(2022)0495 - C9-0322/2022 - 2022/0302(COD)). El texto que utilizaremos en este trabajo es el de esta reciente Resolución; en particular, el texto COR01- Corrección de errores de la Posición del Parlamento Europeo aprobada en primera lectura el 12 de marzo de 2024 con vistas a la adopción de la Directiva (UE) 2024/... del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo (COM(2022)0495; C9-0322/2022;2022/0302(COD)). Disponible en: [https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-12/0132/P9_TA\(2024\)0132\(COR01\)_ES.pdf](https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-12/0132/P9_TA(2024)0132(COR01)_ES.pdf)

³ Hedderich DM, Weisstanner C, Van Cauter S, Federau C, Edjlali M, Radbruch A, et al. "Artificial intelligence tools in clinical neuroradiology: essential medico-legal aspects", *Neuroradiology*, vol. 65, 2023, pp. 1091-1099; Omiye JA, Gui H, Daneshjou R, Cai ZR, Muralidharan V. "Principles, applications, and future of artificial intelligence in dermatology", *Frontiers in Medicine*, vol. 10, 2023; Yousif M, Pantanowitz L. "Artificial intelligence-enabled gastric cancer interpretations: Are we there yet?" *Surgical Pathology Clinics*, vol. 16, núm. 4, 2023, pp. 673-686.

⁴ Khurshid S. "Clinical perspectives on the adoption of the artificial intelligence-enabled electrocardiogram", *Journal of Electrocardiology*, vol. 81, 2023, pp. 142-145.

⁵ Fundación Instituto Roche. Informe Anticipando: *Aplicaciones de la Inteligencia Artificial en Medicina Personalizada de Precisión*, 2023, p. 7.

robótica⁶; el desarrollo de medicamentos⁷; la predicción del riesgo de complicaciones en pacientes hospitalizados⁸, etc.

Por tanto, la IA tiene un gran potencial para mejorar las actuales capacidades de diagnóstico, predicción y pronóstico en medicina y asistencia sanitaria. Ya está realizando grandes avances en el análisis de imágenes, en el desarrollo de medicamentos y sirve de ayuda para enjuiciar y evaluar determinados casos clínicos (relacionados, por ejemplo, con el diagnóstico de diabetes y otras condiciones⁹, la detección temprana de hemorragias cerebrales, etc.)¹⁰. Si a esto sumamos, entre otros avances, la cirugía robótica asistida por IA y los progresos en medicina personalizada, resulta fácil inferir el optimismo que actualmente supone el desarrollo de la IA en salud.

Asimismo, la introducción de la IA en la práctica médica plantea cuestiones jurídicas importantes, cuya complejidad, en ciertos casos, se corresponde con la que caracteriza a estas tecnologías. En la práctica médica los sistemas de IA pueden utilizarse como soporte para la toma de decisiones clínicas, asistiendo a los profesionales médicos a la hora de diagnosticar enfermedades o decidir el tratamiento de pacientes. Su uso como herramientas para estos fines médicos, genera preocupación al caracterizarse ciertos sistemas de IA por su opacidad y complejidad. Pues, esto, entre otros aspectos, dificulta la interpretación y explicación de cómo el sistema ha llegado a los resultados de salida presentados. Por otra parte, los sistemas de IA han podido basar su entrenamiento y aprendizaje en conjuntos de datos incompletos o que no cuentan con la calidad requerida o, incluso, pueden volverse incompletos ante la aparición de nuevos tipos de patologías que eran desconocidos en el momen-

⁶ Morris MX, Song EY, Rajesh A, Asaad M, Phillips BT. "Ethical, legal, and financial considerations of artificial intelligence in surgery", *The American Surgeon*, 2023, vol 89, núm. 1, pp. 55-60.

⁷ Debleena P, Gaurav S, Snehal S, et. al., "Artificial intelligence in drug discovery and development", *Drug Discov Today*, vol. 26, núm. 1, 2021, pp. 80-93.

⁸ Ngiam KY, Khor IW. "Big data and machine learning algorithms for health-care delivery", *The Lancet Oncology*, 2019, vol. 20, núm. 5, pp. e262-e273.

⁹ Un equipo de investigadoras, desarrollaron un algoritmo inteligente, a partir de una serie de variables que comprenden datos médicos, (antecedentes familiares, biopsias pasadas, informes de la patología, etc.), así como otros más generales, (la etnia, la edad de la menopausia, etc.), que logró mejorar una herramienta dirigida a detectar el cáncer de mama. Las pruebas preliminares mostraron una tasa de aciertos del 97% en el diagnóstico de tumores de mama malignos. Gracias a ello, se logró reducir el número de intervenciones innecesarias en, al menos, el 30% con respecto a las aproximaciones anteriores. Véase De Miguel Berian, I. "Medicina personalizada, algoritmos predictivos y utilización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos", *Dilemata*, núm. 30, 2019, pp. 93-109; p. 96.

¹⁰ Dankwa-Mullan I, Rivo M, Sepulveda M, Park Y, Snowdon J, Rhee K. "Transforming Diabetes Care Through Artificial Intelligence: The Future Is Here", *Popul Health Manag*, 2019, vol. 22, núm. 3, pp. 229-242; Akay EMZ, Hilbert A, Carlisle BG, Madai VI, Mutke MA, Frey D. "Artificial Intelligence for Clinical Decision Support in Acute Ischemic Stroke: A Systematic Review", *Stroke*, 2023, vol. 54, núm. 6, pp. 1505-1516.

to de la modelización, etc. Así, puede ocurrir que la patología no aparezca en la imagen debido a un mal funcionamiento del software de procesamiento de imágenes, o ser erróneamente clasificada dados los datos o los parámetros con los que ha sido entrenado el sistema de IA, o debido a que estos datos no presentaban los patrones que caracterizaban a dicha patología concreta, etc.

En este trabajo, no abordaremos la eventual responsabilidad civil del profesional médico que usa un sistema de IA como soporte para la toma de sus decisiones clínicas. Si bien, como señala la RLPEPDRPD, una persona perjudicada podría reclamar, con arreglo al Derecho nacional de los Estados miembros, «una indemnización por daños y perjuicios sobre la base de la responsabilidad contractual o por motivos de responsabilidad extracontractual que no implique la responsabilidad del fabricante por el carácter defectuoso de un producto como se establece en la presente Directiva. Esto afecta, por ejemplo, a la responsabilidad basada en una garantía o en la culpa o la responsabilidad objetiva de los operadores por los daños causados por las propiedades de un organismo resultante de la ingeniería genética. Dichas disposiciones de Derecho nacional, que también sirven para alcanzar, entre otras cosas, el objetivo de una protección eficaz de los consumidores y otras personas físicas, no deben verse afectadas por la presente Directiva»¹¹.

2. EL SISTEMA DE IA COMO PRODUCTO

El sistema de IA utilizado para el diagnóstico basado en imagen médica entra dentro de la delimitación conceptual de «producto» de la RLPEPDRPD. Este es definido como: «cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; incluye la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos» (art. 4.1).

El «sistema de IA» es definido en el artículo 3.1 del Reglamento de Inteligencia Artificial (RIA)¹², en los siguientes términos: «un sistema basado

¹¹ Véase el considerando 9 y el artículo 2.4 de la RLPEPDRPD. Según dispone el art. 2.4.b: «La presente Directiva no afecta a: los derechos que la persona perjudicada tenga en virtud de las normas nacionales en materia de responsabilidad contractual o de responsabilidad extracontractual por motivos distintos del carácter defectuoso de un producto con arreglo a lo dispuesto en la presente Directiva, incluidas las normas nacionales por las que se aplica el Derecho de la Unión».

¹² Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales». Es una definición basada en las principales características de los sistemas de IA que los distinguen de los sistemas de software o los planteamientos de programación tradicionales y más sencillos. Como señala el considerando 12 del RIA, una característica principal de los sistemas de IA es su capacidad de inferencia. Esta se refiere «al proceso de obtención de resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales, y a la capacidad de los sistemas de IA para deducir modelos o algoritmos, o ambos, a partir de información de entrada o datos»¹³.

Asimismo, como señala este considerando, es preciso tener presente que los sistemas de IA «pueden utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente del producto (integrado) o contribuye a la funcionalidad del producto sin formar parte de él (no integrado)».

Precisamente, dadas las características particulares con las que vienen caracterizadas las nuevas tecnologías, se hace manifiesta la necesidad de aclarar el concepto de producto; en particular, con respecto a los programas informáticos¹⁴. Estos no aparecen definidos en la RLPEPDRPD. Hay que acudir al

¹³ Véase el considerando 12 del RIA, en el que asimismo se señala que: «las técnicas que permiten la inferencia al construir un sistema de IA incluyen estrategias de aprendizaje automático que aprenden de los datos cómo alcanzar determinados objetivos y estrategias basadas en la lógica y el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización. El término «basado en una máquina» se refiere al hecho de que los sistemas se ejecutan en máquinas. Estos sistemas pueden funcionar con arreglo a objetivos definidos explícitos o a objetivos implícitos. (...) los resultados de salida generados por el sistema de IA reflejan las distintas funciones desempeñadas por los sistemas e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA puede mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso». Véase el considerando 12 en el que se examinan los términos de la definición señalada en el artículo 3.1 del RIA.

¹⁴ En este trabajo no haremos referencia a otros elementos que se incluyen en el concepto de producto, como, por ejemplo, los archivos de fabricación digital. El «archivo de fabricación digital» es definido como: «una versión digital o plantilla digital de un bien mueble, que contiene la información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas [por ejemplo, impresoras 3D] (art. 4.2 de la RLPEPDRPD). La razón para considerarlos como productos es garantizar la protección de las personas físicas en los casos

considerando 13 que, sin definirlos, nos señala como ejemplos, los siguientes: los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA. Los programas informáticos son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. Dichos programas informáticos pueden introducirse en el mercado como productos autónomos o¹⁵, posteriormente, pueden integrarse en otros productos como componentes¹⁶, y pueden causar daños por su ejecución. Por consiguiente, resultaba ineludible que, en aras de la seguridad jurídica, se aclarase en la nueva Directiva que los programas informáticos son un producto a efectos de la aplicación de la responsabilidad objetiva. Esto con independencia de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo, se accede a él a través de una red de comunicaciones o tecnologías en la nube o se suministra a través de un modelo de programa informático como servicio¹⁷.

en que dichos archivos sean defectuosos. Por ejemplo, un archivo de diseño defectuoso asistido por ordenador, suministrado en el transcurso de una actividad comercial, que cree un bien impreso en 3D que cause daños, dará lugar a la aplicación de este régimen de responsabilidad. Asimismo, las materias primas y la electricidad son productos.

¹⁵ Por ejemplo, el software como producto sanitario (SaMD, por sus siglas en inglés), “se define como el software destinado a ser utilizado para uno o más fines médicos, que lleva a cabo estos fines sin formar parte de un dispositivo médico de hardware”. International Medical Device Regulators Forum, *Software as a Medical Device (SaMD): Key Definitions*, 2013, p. 6. Disponible en: <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>. Un ejemplo de SaMD es el software con un fin médico determinado, que funciona en una plataforma hardware convencional (ordenador, móvil). Pensemos, por ejemplo, en un software destinado al diagnóstico de una enfermedad. Otro ejemplo de SaMD sería una aplicación móvil con fines médicos. Pensemos, por ejemplo, en una aplicación terapéutica de insulina utilizada por un paciente. Es posible que esta pueda cometer un fallo o un error. En este caso, el paciente podría sufrir colapsos hipoglucémicos o hiperglucémicos potencialmente mortales. Véase <https://www.aemps.gob.es/informa/informacion-sobre-la-posibilidad-de-obtener-recomendaciones-de-dosis-de-insulina-incorrectas-al-utilizar-la-funcion-mentor-de-insulina-de-la-aplicacion-movil-onetouchreveal/>. En este enlace la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) señala que: “ha tenido conocimiento, a través de la empresa LifeScan Spain, S.L.U., España, de que la función Mentor de Insulina™, de la aplicación móvil OneTouchReveal, fabricada por LifeScan Europe GmbH, Suiza, pueda proporcionar recomendaciones de dosis de insulina incorrectas. De acuerdo con la información facilitada por la empresa, no han recibido notificaciones de daños relacionados con el uso de esta aplicación móvil. No obstante, como medida de precaución, ha eliminado la configuración individualizada de Mentor de Insulina™ de las aplicaciones de los pacientes afectados”. En noviembre de 2019 el Medical Devices coordination group (MDCG) publicó la siguiente guía: MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 - MDR and Regulation (EU) 2017/746 - IVDR. En esta guía se delimitan los criterios, basándose en la normativa aplicable a la materia, para considerar a determinadas apps como productos sanitarios.

¹⁶ El software como componente integrado en un producto sanitario (SiMD, por sus siglas en inglés). El programa informático puede servir para manejar un producto o tener influencia en su utilización. Pensemos, por ejemplo, en un software que es utilizado para controlar un marcapasos. Un software sanitario destinado a controlar un dispositivo sanitario, también se considerará producto sanitario, y tendrá la misma calificación que el dispositivo que controla.

¹⁷ Véase considerando 13 de la RLPEPDRPD.

Sin embargo, la RLPEPDRPD, según se infiere del citado considerando 13, señala que: «la información no debe considerarse un producto, por lo que las normas sobre responsabilidad por productos defectuosos no deben aplicarse al contenido de los archivos digitales, como los archivos multimedia o los libros electrónicos o el mero código fuente de los programas informáticos»¹⁸. Tampoco es aplicable este régimen de responsabilidad por productos defectuosos, según señala el considerando 14, a los programas informáticos libres y de código abierto desarrollados o suministrados fuera de una actividad comercial (art. 2.2), puesto que los productos así desarrollados o suministrados no se introducen en el mercado, por definición¹⁹. El desarrollo o la contribución a dichos programas informáticos no debe entenderse como su comercialización²⁰. Entre las principales razones que justifican esta exclusión está la no obstaculización de la investigación e innovación²¹. Sin embargo, «cuando los programas informáticos se suministran a cambio de un precio o

¹⁸ Como señala el Tribunal de Justicia de la Unión Europea (TJUE), la información no puede considerarse un producto defectuoso. Caso C-65/20, Sentencia del TJUE (Sala primera) de 10 de junio de 2021 Caso VI contra Krone, ECLI:EU:C:2021:471. En esta sentencia se plantea la cuestión relativa a si un consejo de salud inexacto (referente a la utilización de una planta) incluido en un periódico impreso y que había provocado daños a la salud de un lector, confería a dicho periódico el carácter defectuoso al haberse incorporado al mismo. El TJUE considera que no existe responsabilidad por producto defectuoso ya que el consejo inexacto no se refiere al periódico impreso que constituye su soporte. Se trata de un servicio que no forma parte de los elementos intrínsecos al periódico impreso que son los únicos que permitirían apreciar si dicho producto es defectuoso. Véase Navas Navarro, S. *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022, p. 85; Koch AB, et. al. “Response of the European Law Institute to the Public Consultation on Civil Liability - Adapting Liability Rules to the Digital Age and Artificial Intelligence”, *Journal of European Tort Law*, vol. 13, 1, 2022, pp. 25-63; p. 35; Howells, G., Twigg-flesner, Ch., Willett Ch. “Product Liability and Digital Products”, in Synodinou, TE., Jouglex, P., Markou, Ch., Prastitou, T. *EU Internet Law. Regulation and Enforcement*, Springer, 2017, pp. 183-195; p.189; Ataz López, J. *Daños causados por las cosas: Una nueva visión a raíz de la robótica y de la inteligencia artificial*. Working paper 4/2020, pp. 1-58; p. 35; Atienza Navarro, ML. “¿Una nueva responsabilidad por productos defectuosos?”, *Indret*, 2.2023, pp. 1-53; pp. 11-12.

¹⁹ La «introducción en el mercado» es definida como: «primera comercialización de un producto en el mercado de la Unión» (art. 4.8 de la RLPEPDRPD). La «comercialización» es definida como: «todo suministro, ya sea a título oneroso o gratuito, de un producto para su distribución, consumo o utilización en el mercado de la Unión en el transcurso de una actividad comercial» (art. 4.7). Y, la «puesta en servicio» se define en los siguientes términos: «la primera utilización de un producto en la Unión en el transcurso de una actividad comercial ya sea a título oneroso o gratuito, en circunstancias en las que el producto no se haya introducido en el mercado antes de su primera utilización» (art. 4.9).

²⁰ Según el considerando 14 RLPEPDRPD: «No debe considerarse como comercialización el suministro de este tipo de programas en repositorios abiertos, a menos que ello se dé en el transcurso de una actividad comercial».

²¹ «Los programas informáticos libres y de código abierto por los que el código fuente se comparte abiertamente y los usuarios pueden acceder, utilizar, modificar y redistribuir libremente los programas informáticos o sus versiones modificadas, pueden contribuir a la investigación y la innovación en el mercado. Estos programas informáticos están sujetos a licencias que garantizan a todos la libertad de ejecutarlos, copiarlos, distribuirlos, estudiarlos, cambiarlos y mejorarlos» (considerando 14).

de datos personales para cualquier otro fin que no sea exclusivamente el de mejorar la seguridad, la compatibilidad o la interoperabilidad del programa informático y, por tanto, se suministren en el transcurso de una actividad comercial, debe aplicarse la presente Directiva» (considerando 14).

Por otra parte, es preciso tener presente que: «cuando dichos programas informáticos libres y de código abierto suministrados fuera de una actividad comercial sean posteriormente integrados por un fabricante como componente en un producto en el transcurso de una actividad comercial y, por tanto, se introduzcan en el mercado, debe ser posible considerar a dicho fabricante responsable de los daños causados por el carácter defectuoso de dichos programas, *pero no así al fabricante de los programas puesto que este no habría cumplido las condiciones de introducción en el mercado de un producto o componente*» (considerando 15). Con el subrayado destacamos la idea de que faltaría en dicho fabricante del programa la actividad comercial que se requiere en los sujetos responsables para la aplicación de este régimen de responsabilidad²². De hecho, si el programa hubiese sido suministrado a cambio de un precio y el fabricante lo integrase en su producto, en el caso de que este ocasionase daños debido a que aquel era defectuoso, la persona perjudicada podrá reclamar una indemnización tanto al fabricante que integró el programa en su producto como al fabricante de dicho programa defectuoso. Para garantizar la protección de las personas físicas, todas las partes deben ser consideradas responsables solidariamente en tales situaciones²³.

Una vez examinado que el sistema de IA utilizado para el diagnóstico basado en imagen médica entra dentro del concepto de producto propuesto en la RLPEPDRPD, es preciso preguntarse, en aras de conocer qué normativa resulta aplicable, si este puede considerarse como un «producto sanitario» y como un «sistema de IA de alto riesgo».

3. EL SISTEMA DE IA COMO PRODUCTO SANITARIO

El sistema de IA que se utiliza como soporte para la toma de decisiones clínicas (por ejemplo, para diagnóstico, prevención, seguimiento, predicción, prognosis o tratamiento), entra dentro de la delimitación conceptual de «pro-

²² En este trabajo no haremos referencia a los distintos sujetos responsables. La RLPEPDRPD amplía el abanico de operadores económicos que pueden ser considerados responsables de los productos defectuosos. Véase, más ampliamente, Jorqui Azofra, M. *Responsabilidad por los daños causados por productos defectuosos y sistemas de inteligencia artificial*, en Moreno Martínez, JA. (Dir.), Dykinson, Madrid, 2023, pp. 203-233.

²³ Como veremos, la RLPEPDRPD establece que, cuando dos o más operadores económicos sean responsables de los mismos daños, puedan ser considerados responsables solidariamente (art. 12.1).

ducto sanitario», dado que es utilizado en personas con un fin médico específico según lo dispuesto en el artículo 2.1 del Reglamento (UE) 2017/745 sobre los productos sanitarios²⁴. Por otra parte, según señala el RIA, dado que dicho producto sanitario requiere someterse a un procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros de acuerdo con dicho Reglamento (UE) 2017/745 (acto legislativo de armonización de la Unión, incluido en el anexo I del RIA)²⁵, es considerado como un sistema de IA de alto riesgo²⁶.

Según el Reglamento (UE) 2017/745, para obtener el marcado CE²⁷, el producto ha de someterse a un procedimiento de evaluación de la conformidad que viene determinado en función de la clasificación de dicho producto²⁸. Los productos sanitarios se clasifican, según su finalidad prevista y los riesgos inherentes, en las clases I, IIa, IIb, y III, según lo establecido en el

²⁴ Reglamento (UE) 2017/745 del Parlamento europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo. El artículo 2.1 del citado Reglamento define como «producto sanitario»: todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos:

- diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad,
- diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad,
- investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico,
- obtención de información mediante el examen *in vitro* de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos, y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos».

²⁵ Véase la definición de «organismo de evaluación de la conformidad» establecida por el art. 2.40 del Reglamento 2017/745, con arreglo al cual este es definido como: «un organismo independiente que desempeña actividades de evaluación de la conformidad como calibración, ensayo, certificación e inspección». Un «organismo notificado» es definido como: «un organismo de evaluación de la conformidad designado con arreglo al presente Reglamento (art. 2.41). Véase, asimismo, las definiciones dadas por el RIA en el art. 3, apartados 21 y 22, respectivamente.

²⁶ Véase considerando 50 del RIA, así como el art. 6, que contiene las «Normas de clasificación de los sistemas de IA de alto riesgo» (en particular, el art. 6.1) y el anexo I que recoge la «Lista de actos legislativos de armonización de la Unión», en el que está incluido el Reglamento (UE) 2017/745 sobre los productos sanitarios (Sección A. 11).

²⁷ El «marcado CE de conformidad» o «marcado CE» es definido como: «un marcado por el que un fabricante indica que un producto es conforme con los *requisitos aplicables establecidos en el presente Reglamento y otra legislación de armonización de la Unión aplicable que prevea su colocación*» (art. 2.43) (el subrayado es nuestro).

²⁸ La «evaluación de la conformidad» es: «el proceso por el que se demuestra si un producto satisface los requisitos del presente Reglamento (art. 2.40 del Reglamento (UE) 2017/745). En el RIA la «evaluación de la conformidad» es definida como: «el proceso por el que se demuestra si se

anexo VIII) (art. 51.1). Dicha clasificación (que establece una escala que va desde la clase I (menor riesgo) hasta la clase III (mayor riesgo) determina de menor a mayor el grado de intervención regulatoria²⁹. «Si el programa informático es independiente de cualquier otro producto, será clasificado por sí mismo»³⁰. A este resulta aplicable la Regla 11 del anexo VIII del Reglamento (UE) 2017/745. De conformidad con lo dispuesto en la misma: «Los programas informáticos destinados a proporcionar información que se utiliza para tomar decisiones con fines terapéuticos o de diagnóstico se clasifican en la clase IIa, salvo si estas decisiones tienen un impacto que pueda causar: - la muerte o un deterioro irreversible del estado de salud de una persona, en cuyo caso se clasifican en la clase III, o - un deterioro grave del estado de salud de una persona o una intervención quirúrgica, en cuyo caso se clasifican en la clase IIb»³¹.

En este sentido, tratándose de un sistema de IA utilizado para el diagnóstico basado en imagen médica, ha de someterse, según lo señalado, al Reglamento (UE) 2017/745 y ha de cumplir con los requisitos establecidos por el RIA para los sistemas de IA de alto riesgo (sección 2 del Capítulo III del RIA)³². El sistema de IA que se usa para el diagnóstico basado en imagen

han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo» (art. 3.20).

²⁹ Lazcoz Moratinos, G. *Sistemas de inteligencia artificial en la asistencia sanitaria: cómo garantizar la supervisión humana desde la normativa de protección de datos*: <https://www.aepd.es/documento/premio-emilio-aced-2022-guillermo-lazcoz.pdf>

³⁰ Véase Regla 3.3, segundo párrafo, del anexo VIII del Reglamento (UE) 2017/745. En el caso de que un programa informático sirva para manejar un producto o tenga influencia en su utilización se incluirá en la misma clase que el producto, según señala la Regla 3.3, primer párrafo, del citado Reglamento.

³¹ En general el sistema de IA utilizado para el diagnóstico, será clasificado en la clase IIa. Véase, por ejemplo, Quaranta, M, Amantea, IA y Grosso, M. “Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double?”, *The Review of Socionetwork Strategies*, vol. 17, 2013, pp. 275-295; pp. 287-288. Los autores señalan que DeepHealth para el diagnóstico del cáncer de pulmón (aplicación de IA desarrollada en el marco de un proyecto europeo llamado DeepHealth), tiene como función “ayudar en el diagnóstico”; esto es, sus resultados de salida sirven de soporte a los profesionales médicos en su proceso de toma de decisiones. Dado que las tareas establecidas como objetivos de dicha aplicación de IA son exámenes de imágenes, la detección de nódulos y proporcionar apoyo a los profesionales médicos, se clasifica bajo la clase IIa del Reglamento (UE) 2017/745. Como señalan los autores, se trata de un sistema de IA de alto riesgo y un producto sanitario de clase IIa. Los fabricantes de esta aplicación de IA deberán cumplir con las obligaciones correspondientes de la normativa aplicable, con obligaciones *ex ante* (antes de su introducción en el mercado o puesta en servicio), durante su ciclo de vida en el mercado y con obligaciones postcomercialización. Los fabricantes de la aplicación deben cumplir con los requisitos correspondientes establecidos tanto en el Reglamento (UE) 2017/745 como en el RIA.

³² Hay dispositivos médicos basados en IA que se utilizan, por ejemplo, para realizar un cribado de retinopatía diabética. Véase Grzybowski, A., Brana, P., Lim, G., et. al. “Artificial intelligence for diabetic retinopathy screening: a review”, *Eye*, vol. 34, 2020, pp. 451-460. Los peores desenlaces de retinopatía diabética (RD) se pueden prevenir mediante la implementación de programas de cri-

médica puede presentar riesgos de los que no se ocupen los requisitos de salud y seguridad establecidos en la legislación sectorial, ya que el Reglamento (UE) 2017/745 no aborda los riesgos específicos de los sistemas de IA. Precisamente, el RIA, con el fin de mitigar los riesgos de los sistemas de IA de alto riesgo, y para garantizar un alto nivel de fiabilidad, establece que a estos deben aplicarse ciertos requisitos obligatorios que tengan en cuenta la finalidad prevista y el contexto del uso del sistema³³. Así, el sistema de IA utilizado

bado de RD, que pueden beneficiarse del uso de un dispositivo médico basado en IA. En el Hospital Universitario de Navarra (HUN), un equipo de profesionales médicos evalúa imágenes de fondo de ojo para derivar al especialista (oftalmólogo) a los pacientes que podrían ser citados para un examen ocular presencial. En el Servicio Navarro de Salud se estudia esta posibilidad de incluir una herramienta basada en IA; esto es, un software de cribado de la retinopatía diabética (RD) basado en IA, (denominado NaIA-RD). Este está integrado en la historia clínica informatizada (HCI) del HUN. En un estudio piloto se está utilizando NaIA-RD para el cribado de la RD en un circuito en el que los cribadores (médicos de Atención Primaria) han visualizado todas las retinografías acompañadas de una propuesta procedente de la IA. En un segundo nivel de cribado (donde intervienen oftalmólogos) se pretende que estos, haciendo uso de la HCI: validen en lote las prestaciones de retinografía que NaIA-RD valora como no referibles. Se trata de que el oftalmólogo tenga “la posibilidad de visualizar las que estime oportunas (por ejemplo, aquellas donde NaIA-RD tiene más incertidumbre). El informe que se remite al médico de cabecera incluye la información [detallada] sobre la escala de severidad internacional (ICDR) [no retinopatía diabética, leve, moderada, severa o proliferativa] que aporta NaIA-RD”. Asimismo, el oftalmólogo “visualiza todas las prestaciones de retinografía que NaIA-RD ha valorado como referibles para tomar la decisión final de cribado. Puede aceptar las recomendaciones de NaIA-RD para agilizar la generación de informes, que incluirán la información detallada ICDR. En ambos escenarios, el oftalmólogo genera informes validados y firmados por él, que se envían de forma automática al médico de cabecera del paciente”. Estudio en desarrollo que se basa fundamentalmente en el siguiente trabajo: Pinto, Imanol and Olazarán, Álvaro and Jurío, David and de la Osa, Borja and Sainz, Miguel and Oscoz, Aritz and Ballaz, Jerónimo and Gorricho, Javier and Galar, Mikel and Andonegui, José, “Improving Diabetic Retinopathy Screening Using Artificial Intelligence: Design, Evaluation and Before-and-After Study of an In-House Development”. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.4744622>.

³³ Deben aplicarse a los sistemas de IA de alto riesgo los siguientes requisitos: Se establecerá, implantará, documentará y mantendrá un *sistema de gestión de riesgos* durante todo el ciclo de vida del sistema (art. 9); cuando se utilicen técnicas que impliquen el entrenamiento de modelos de IA con datos, los sistemas se desarrollarán a partir de conjuntos de *datos* de entrenamiento, validación y prueba que cumplan los correspondientes criterios de calidad en aras de cumplir con las pertinentes obligaciones relativas a los *datos y gobernanza de datos* (art. 10); se elaborará la *documentación técnica* que permita demostrar el cumplimiento de los requisitos legalmente exigidos por el RIA (art. 11); se establecerá un *registro automatizado* («archivos de registro») para garantizar la trazabilidad del funcionamiento del sistema a lo largo de todo su ciclo de vida (art. 12); se cumplirá con las correspondientes obligaciones de *transparencia y comunicación* de información a los responsables del despliegue para garantizar una interpretación y uso correcto de los resultados de salida del sistema (art. 13); se cumplirá con las respectivas obligaciones de *supervisión humana* para garantizar que los sistemas sean diseñados y desarrollados de forma que puedan ser supervisados de manera efectiva por personas físicas durante todo el período que estén en uso (art. 14); se cumplirá con las obligaciones referentes a alcanzar un nivel adecuado de *precisión, solidez y ciberseguridad* de manera que los sistemas funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida (art. 15). Dichos requisitos, como señala el considerando 66 del RIA, «son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales».

para el diagnóstico basado en imagen médica solo puede introducirse en el mercado o ponerse en servicio cuando cumpla con lo dispuesto en el RIA y con la legislación de armonización de la Unión que sea aplicable. Como norma general, diversos actos legislativos pueden resultar aplicables simultánea y complementariamente³⁴.

Para reducir la carga que soportaría el proveedor de dicho sistema de IA y evitar posibles duplicidades, conviene que la conformidad de dicho sistema con los requisitos establecidos en el RIA se evalúe en el marco de la evaluación de la conformidad ya prevista en el Reglamento (UE) 2017/745 (considerando 124 del RIA). Con arreglo a lo dispuesto en el artículo 43.3 del RIA, al tratarse, en nuestro caso, de un sistema de IA de alto riesgo regulado por el Reglamento (UE) 2017/745, el proveedor se someterá al procedimiento de evaluación de la conformidad pertinente exigido por dicho Reglamento sobre los productos sanitarios. Los requisitos establecidos en la sección 2 del Capítulo III del RIA se aplicarán a dicho sistema de IA que se use para el diagnóstico basado en imagen médica y formarán parte de dicha evaluación. «Asimismo, se aplicarán los puntos 4.3, 4.4 y 4.5 del anexo VII [del RIA], así como el punto 4.6, párrafo quinto, de dicho anexo» (art. 43.3 del RIA). A efectos de dicha evaluación, según dispone el artículo 43.3 del RIA, «los organismos notificados que hayan sido notificados con arreglo a dichos actos legislativos dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en la sección 2, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11, en el contexto del procedimiento de notificación con arreglo a dichos actos legislativos»³⁵.

Por consiguiente, el sistema de IA utilizado para el diagnóstico es un producto sanitario (en general, clasificado como clase IIa o superior), y un sistema de IA de alto riesgo, por lo que tendrá que demostrar, también, que cumple con los requisitos obligatorios establecidos para estos (arts. 9 a 15 del RIA). El cumplimiento de estos y de los pertinentes requisitos de seguridad establecidos en el Reglamento (UE) 2017/745, será fundamental para apreciar si el sistema de IA es, en su caso, defectuoso. Precisamente, entre las circunstancias relevantes para valorar si un producto es de carácter defectuoso, se tendrá en cuenta, como veremos, «los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad» (art. 7.2.f de la RLPEPDRPD).

³⁴ Por ejemplo, si el sistema de IA de alto riesgo y producto sanitario utiliza datos personales de los pacientes, habrá de cumplir también con lo dispuesto en el RGPD.

³⁵ En el art. 31 del RIA se establecen los requisitos relativos a los organismos notificados. Entre estos hay que tener presente que serán independientes del proveedor del sistema de IA de alto riesgo en relación con el cual lleven a cabo actividades de evaluación de la conformidad.

Asimismo, la demostración de que un producto no cumple con los requisitos obligatorios de seguridad establecidos en la normativa aplicable es una de las condiciones que dicha RLPEPDRPD prevé para proceder, en su caso, a la presunción del carácter defectuoso del producto.

4. ¿QUÉ DETERMINA EL CARÁCTER DEFECTUOSO DEL SISTEMA DE IA?

La noción de «seguridad» es el elemento clave para determinar la existencia de «defecto» en la RLPEPDRPD³⁶. El artículo 7 establece que: «un producto se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional»³⁷. La valoración del carácter defectuoso de un producto ha de incluir un análisis objetivo de la seguridad que el público en general tiene derecho a esperar y no referirse a la seguridad que una persona concreta tiene derecho a esperar. Desde este enfoque de las expectativas de seguridad que legítimamente cabe esperar por el público en general, la RLPEPDRPD amplía (sin ser una lista cerrada) el número de circunstancias que deberán tenerse en cuenta a la hora de valorar el carácter defectuoso de un producto³⁸. Destacaremos algunas de ellas en función de algunas características propias de nuestro producto sanitario que es también un sistema de IA de alto riesgo.

Entre dichas circunstancias sigue figurando la presentación del producto, sus características, incluidas las técnicas, su etiquetado, diseño, composición y envase, y las instrucciones de montaje, instalación, uso y mantenimiento (art. 7.2.a)³⁹. En general, la presentación del producto hace referencia a aquellos aspectos que tienen que ver con la confianza que suscita el fabricante que

³⁶ La doctrina, en general, coincide al señalar que el elemento sobre el que se basa el concepto de «defecto» es la «seguridad». Véase, entre otros, Solé Feliu, J. *El concepto de defecto del producto en la responsabilidad civil del fabricante*, Tirant lo Blanch, Valencia, 1997, p. 574; Marín López, J.J. *Daños por productos: estado de la cuestión*, Tecnos, Madrid, 2001, p. 28; Gutiérrez Santiago, P. *Daños causados por productos defectuosos*, Aranzadi, Cizur Menor, 2008, pp. 79-81.

³⁷ El carácter defectuoso del producto viene determinado no por su falta de aptitud para el uso sino por no cumplir las correspondientes condiciones de seguridad. La falta de calidad, de conformidad o de idoneidad del producto para el uso previsto se regirá, en su caso, por aplicación del régimen de garantías y no por este régimen de responsabilidad civil.

³⁸ Véase lo dispuesto en el art. 7.2 de la RLPEPDRPD.

³⁹ En el Reglamento (UE) 2017/745 las «instrucciones de uso» son definidas como: «la información facilitada por el fabricante para informar al usuario sobre la finalidad prevista de un producto, su uso correcto y las precauciones que deban tomarse» (art. 2.14). En el RIA estas son definidas como: «la información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA» (art. 3.15).

introduce el producto en el mercado⁴⁰. En este sentido, ha de ser completa, correcta y clara; esto es, no puede inducir a ningún tipo de error⁴¹. Pues, a partir de la presentación del producto se crean expectativas de seguridad en relación con su uso. En el anexo I del Reglamento (UE) 2017/745 se establecen los requisitos generales de seguridad y funcionamiento de los productos⁴². La demostración de la conformidad con dichos requisitos generales deberá incluir una evaluación clínica con arreglo al artículo 61 (art. 5.3)⁴³. Entre dichos requisitos se incluye la obligación del fabricante de establecer, aplicar, documentar y mantener un sistema de gestión de riesgos durante el ciclo de vida del producto en aras de proteger la seguridad y la salud de las personas (Capítulo I, anexo I); se señala que este ha de diseñarse y fabricarse de modo que se garantice que las características y requisitos de funcionamiento establecidos en el Capítulo I se cumplen. En cuanto a los productos de diagnóstico, estos han de diseñarse de manera que proporcionen exactitud, precisión y constancia suficientes para la finalidad prevista, sobre la base de métodos científicos y técnicos adecuados. Los límites de la exactitud han de ser indicados por el fabricante⁴⁴; asimismo, en el citado anexo I se indican

⁴⁰ En varias sentencias, quedan integrados, dentro de este elemento de la «presentación», la información ofrecida por el fabricante sobre el uso y características del producto. Por ejemplo, SSAAPP de Barcelona de 27 de septiembre de 2006 (AC 2006/1724), de 17 de diciembre de 2001 (JUR 2002/84388), de Cáceres de 18 de abril de 2002 (AC 2002/1330). Se trata de examinar cómo el operador económico presenta el producto, lo describe y enumera sus características, cualidades y funcionalidades.

⁴¹ Véase el artículo 7 del Reglamento (UE) 2017/745, donde se prohíbe el uso de signos que puedan inducir a error al usuario o al paciente en cuanto a la finalidad prevista, la seguridad y el funcionamiento del producto por alguno de los siguientes medios: atribuir al producto funciones y propiedades que no posee; crear una falsa impresión sobre tratamiento o diagnóstico, funciones o propiedades que el producto no posee; no informar al usuario o al paciente sobre los posibles riesgos que conlleva la utilización del producto conforme a su finalidad prevista; dar a entender usos del producto diferentes a los indicados como parte de la finalidad prevista para la que se realizó la evaluación de la conformidad.

⁴² Véase artículo 5.2 del citado Reglamento donde se establece que: «Los productos sanitarios cumplirán los requisitos generales de seguridad y funcionamiento que figuran en el anexo I que les sean aplicables, teniendo en cuenta su finalidad prevista».

⁴³ El fabricante especificará y justificará el nivel de las pruebas clínicas necesario para demostrar la conformidad con los requisitos generales de seguridad y funcionamiento. Asimismo, dicho nivel de pruebas clínicas será el adecuado en atención a las características del producto y su finalidad prevista. La correspondiente evaluación clínica deberá estar debidamente documentada (con arreglo al art. 61 y a la parte A del Anexo XIV del Reglamento (UE) 2017/745). La «evaluación clínica» es: «un proceso sistemático y planificado para generar, recoger, analizar y evaluar de forma continua los datos clínicos relativos a un producto para verificar su seguridad y funcionamiento, incluidos los beneficios clínicos, cuando se utilice conforme a la finalidad prevista por el fabricante» (art. 2.44 del Reglamento (UE) 2017/745).

⁴⁴ Véase el Capítulo II del anexo I, apartado 15.1 También, para los programas informáticos que constituyan productos por sí mismos, estos se desarrollarán y fabricarán basándose en el estado actual de la técnica, teniendo en cuenta los principios de ciclo de vida del desarrollo, gestión de los riesgos, incluida la seguridad de la información, validación y verificación (apartado 17.2 del Capítulo II, anexo I).

los requisitos generales en relación con la información que ha de facilitar el fabricante. Se establece que los productos deben ir acompañados de la información necesaria para identificar el producto y a su fabricante, y de información pertinente sobre la seguridad y funcionamiento para el usuario o cualquier otra persona, según proceda. En el Capítulo III del anexo I se especifica qué información ha de figurar, entre otros elementos, en las instrucciones de uso⁴⁵. Por otra parte, la documentación técnica que ha de elaborar el fabricante, y que permitirá que se evalúe la conformidad del producto con los requisitos del Reglamento (UE) 2017/745, contendrá los elementos que se especifican en los anexos II y III⁴⁶.

Tratándose de un producto sanitario que es un sistema de IA de alto riesgo ha de cumplir asimismo con los requisitos pertinentes exigidos por el RIA a estos efectos (arts. 9 a 15). Estos completarán el conjunto de los requeridos por el Reglamento (UE) 2017/745. Así, se contempla, por ejemplo, la obligación de llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA en cuestión cumple dichos requisitos previstos en el RIA y facilitar la vigilancia poscomercialización⁴⁷. En general, dicha información ha de incluir las características generales, las capacidades y las limitaciones del sistema de IA y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos correspondiente, elaborada de manera clara y completa. La documentación técnica del sistema de IA ha de elaborarse antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada. «Contendrá, como mínimo, los elementos contemplados en el anexo IV de manera simplificada» (art. 11.1 del RIA)⁴⁸.

⁴⁵ Capítulo III del anexo I, apartado 23.4.

⁴⁶ En el anexo II se señalan como elementos que ha de incluir la documentación técnica aquellos referidos a: la descripción y especificaciones del producto; la información que debe facilitar el fabricante; la información sobre diseño y fabricación; los requisitos generales de seguridad y funcionamiento; el análisis de beneficios y riesgos y gestión de riesgos; y la verificación y validación de los productos. En el anexo III se recogen los elementos que han de figurar en la documentación técnica sobre seguimiento poscomercialización.

⁴⁷ Véase el artículo 11, considerando 71 y anexo IV del RIA.

⁴⁸ El anexo IV del RIA, establece qué información, como mínimo, ha de incluir la documentación técnica a que se refiere el artículo 11.1. Dentro de lo que se refiere a la descripción general del sistema de IA ha de incluirse, entre otros elementos, los siguientes: Su finalidad prevista; la manera en que el sistema interactúa o puede utilizarse para interactuar con *hardware* o *software*, también con otros sistemas de IA; instrucciones de uso para el responsable del despliegue, etc. En cuanto a la descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, han de incluirse, entre otros factores, los siguientes: los métodos y las medidas adoptados para el desarrollo del sistema de IA; las especificaciones de diseño del sistema; la arquitectura del sistema; cuando proceda, los requisitos en materia de datos; una evaluación de las medidas de supervisión humana; las medidas de ciberseguridad, etc. Asimismo, ha de incluirse información detallada acerca de la supervisión, el funcionamiento y el control del sistema de IA, en particular con respecto a sus capacidades y limitaciones de funcionamiento.

Por otra parte, resulta preciso que el sistema de IA de alto riesgo se diseñe y desarrolle de tal manera que garantice un nivel de transparencia suficiente para que los responsables del despliegue del sistema (la persona física o jurídica que utilice el sistema bajo su autoridad)⁴⁹, interpreten y usen correctamente sus resultados de salida. En este sentido, el sistema, irá acompañado de las instrucciones de uso correspondientes, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue⁵⁰. En general, dicha información hace referencia a las características, las capacidades y las limitaciones del funcionamiento del sistema. Estas comprenderán la información sobre las posibles circunstancias conocidas y previsibles relativas al uso del sistema, incluida la actuación del responsable del despliegue capaz de influir en el comportamiento y funcionamiento del sistema; en particular, cuando pueda dar lugar a riesgos para la salud. También dicha información abarcará los cambios que el proveedor haya predeterminado y evaluado para comprobar su conformidad y las medidas pertinentes de supervisión humana, incluidas aquellas que faciliten la interpretación de los resultados de salida del sistema.

Precisamente, cuando se omite una adecuada información sobre el producto, sobre las condiciones de su uso correcto, el defecto (defecto de información) existe si, de haberse incluido la información omitida, el daño hubiera podido evitarse, pues el usuario hubiera podido evitar actuar de otra forma distinta a como lo hizo⁵¹. Esta consideración ha de tenerse en cuenta: de un

to, incluidos los niveles de precisión para las personas o colectivos de personas específicos en relación con los que está previsto que se utilice el sistema y el nivel general de precisión esperado en relación con su finalidad prevista. También ha de incluirse toda aquella información que abarque los siguientes aspectos: una descripción de la idoneidad de los parámetros de rendimiento para el sistema de que se trate, del sistema de gestión de riesgos, de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida, del sistema establecido para evaluar su funcionamiento en la fase posterior a su comercialización, así como una lista de las normas armonizadas que resulten aplicables, total o parcialmente, y una copia de la declaración de UE de conformidad.

⁴⁹ El responsable del despliegue es definido como: «una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional» (Art. 3.4 del RIA).

⁵⁰ Véase el artículo 13.3 del RIA, en el que se señala qué información, como mínimo, han de incluir las instrucciones de uso.

⁵¹ Véase la SAP de Barcelona de 16 de marzo de 2009 (AC 2009/1534) en la que se aprecia el defecto de un medicamento por no informar su prospecto de todos los efectos secundarios que puede producir. La ausencia o insuficiencia de instrucciones para la adecuada utilización del producto (y, en caso, por ejemplo, de productos potencialmente peligrosos, la falta de advertencia de los posibles riesgos que su uso pudiera provocar), constituyen supuestos de productos defectuosos susceptibles de enmarcarse en el régimen de responsabilidad por daños causados por productos. Véase, por ejemplo, SAP Baleares de 19 de julio de 2000 (JUR 2000/296591); SAP de Barcelona de 17 de diciembre de 2001 (JUR 2002/84388); SAP de Zaragoza de 7 de marzo de 2003 (JUR 2003/110291); SAP Barcelona de 13 de junio de 2005 (JUR 2005/181270); SAP Palencia de 2 de noviembre de 2006 (AC 2006/105); SAP de Asturias de 24 de abril de 2009 (JUR 2009/283840).

lado, para configurar el producto como defectuoso o no; y, de otro lado, para acreditar la relación causal entre el producto calificado como defectuoso y la producción del daño. Desde esta perspectiva, se señala que no es suficiente, para imputar responsabilidad al fabricante, la prueba de que éste ha omitido determinada información, si esta no ha sido la causa del daño sufrido por la persona perjudicada⁵². Tratándose de un sistema de IA que se utiliza para el diagnóstico, las instrucciones de uso han de ser lo suficientemente concisas, completas, correctas, claras, comprensibles, etc., para que los profesionales médicos que lo utilicen puedan tomar sus decisiones con conocimiento de causa. Debe garantizarse, por parte del proveedor del sistema, que dichas instrucciones de uso contengan la información necesaria para saber cómo utilizarlo y cómo interpretar sus resultados de salida (art. 13.3 del RIA), así como el nivel de formación y competencias requeridas para desempeñar la función de supervisión.

Precisamente, las instrucciones de uso resultan esenciales también para examinar qué constituye un «uso razonablemente previsible del producto» (art. 7.2.b de la RLPEPDRPD)⁵³. Al evaluar el carácter defectuoso de un producto, también se incluye en los términos de la valoración el «uso indebido pero razonable en las circunstancias»⁵⁴, como, por ejemplo, «el comportamiento previsible de un usuario de maquinaria derivado de la falta de concentración»⁵⁵. Tratándose de un sistema de IA utilizado para el diagnóstico, debe advertirse del riesgo, entre otros, relativo al denominado «sesgo de automati-

⁵² Parra Lucán, MA. “Artículo 137”, en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentario del texto refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias*, Cizur Menor, Aranzadi, 2015; Ramos González, S. *Responsabilidad civil por medicamento. Defectos de fabricación, de diseño y en las advertencias o instrucciones*, Civitas, Madrid, 2004.

⁵³ Un producto puede definirse como defectuoso cuando no ofrezca la seguridad que el público en general tiene derecho a esperar, (sea a causa de un defecto de fabricación, de diseño, de información, etc.), teniendo en cuenta todas las circunstancias, tales como, entre otras, el uso razonablemente previsible y el uso indebido razonablemente previsible. Así, el fabricante ha de diseñar el producto de forma que resulte seguro con respecto a los usos (incluso no habituales) que entren dentro de lo razonablemente previsible. Véase Jorqui Azofra, M. op. cit., 2023, pp. 195 y ss.

⁵⁴ En el RIA el art. 13.3. b. iii) hace referencia, dentro de la información que ha de comprender las instrucciones de uso, (en particular, con respecto a las características, capacidades y limitaciones del sistema de IA), a la inclusión de: «cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a *un uso indebido razonablemente previsible*, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales». (el subrayado es nuestro).

⁵⁵ Véase el considerando 31 de la RLPEPDRPD, donde se señala que: «las advertencias u otra información proporcionada con un producto no pueden considerarse suficientes para que un producto por lo demás defectuoso sea seguro, ya que el carácter defectuoso debe determinarse en función de la seguridad que el público en general tiene derecho a esperar. Por lo tanto, la responsabilidad con arreglo a la presente Directiva no puede eludirse simplemente enumerando todos los efectos secundarios imaginables de un producto».

zación»; es decir, a «la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por el sistema de IA de alto riesgo» (art. 14.4.b del RIA). Esto es especialmente relevante cuando este se utiliza para aportar información o recomendaciones a fin de que los profesionales médicos adopten una decisión clínica que puede afectar significativamente a la salud de los pacientes⁵⁶.

En este sentido, habrá de valorarse en qué medida la causación del daño ha de imputarse objetivamente a la deficiencia del producto (por ejemplo, a un defecto de información). Si bien, como veremos, el *operador económico* podría alegar⁵⁷, la denominada causa de exoneración de responsabilidad basada en los riesgos del desarrollo (art. 11.1.e de la RLPEPDRPD). Pues, no podrá informar de riesgos que, a la luz del nivel más avanzado de conocimiento objetivo accesible, no era posible examinar y valorar⁵⁸.

Asimismo, habrá de evaluarse en qué medida la causación del daño ha de imputarse objetivamente a alguna deficiencia del producto y/o a un acto u omisión de un tercero, y/o a una actuación negligente de la persona perjudicada (o de una persona de la que esta sea responsable). La RLPEPDRPD se ocupa de la reducción de responsabilidad. Por un lado, impide que la responsabilidad del operador económico se reduzca o anule cuando los daños sean causados tanto por el carácter defectuoso de un producto como por un acto u omisión de un tercero (art. 13.1). Pensemos, por ejemplo, en el supuesto en el que el sistema de IA de alto riesgo presentase una vulnerabilidad de ciberseguridad que, a su vez, es explotada por un tercero para crear un malware causando daños. En este caso, el sistema que presenta dicha vulnerabilidad, (por ejemplo, por no haber cumplido con los requisitos de ciberseguridad requeridos por el RIA)⁵⁹, hace que sea menos seguro de lo que el público en general tiene derecho a esperar. La responsabilidad del operador económico

⁵⁶ Como señala Gil Membrado, C: “Del mismo modo que el profesional valida la aplicación del Protocolo al caso concreto, debe hacerlo cuando la herramienta de apoyo a su decisión esté basada en algoritmos, teniendo en cuenta, además, que el profesional no debe adoptar decisiones basadas únicamente en los perfiles o en las propuestas de decisión de la máquina sin su intervención significativa”. Véase Gil Membrado, C. *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*. VIII Premio Nacional de Derecho Sanitario, Madrid, Reus, 2023, p. 174.

⁵⁷ El «operador económico» en la RLPEPDRPD es definido como: «todo fabricante de un producto o componente, prestador de un servicio conexo, representante autorizado, importador, prestador de servicios logísticos o distribuidor» (art. 4.15 de la RLPEPDRPD). En el RIA el «operador» se define como: «un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor» (art. 3.8).

⁵⁸ Véase Navas Navarro, S. *Daños ocasionados...*, op. cit., 2022, pp. 92 y 93.

⁵⁹ Véase art. 15.5 del RIA, considerandos 76, 77 y 78. La ciberseguridad es esencial para garantizar que el sistema de IA resista a las actuaciones de terceros maliciosos que, aprovechando vulnerabilidades del sistema, traten de alterar su uso, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad.

no debe reducirse o anularse como consecuencia de tales actos u omisiones de un tercero⁶⁰. Se mantiene, en estos supuestos, la posibilidad de ejercer, a la luz de lo que indique el Derecho nacional, el derecho de repetición.

Por otro lado, debe ser posible reducir o anular la responsabilidad del operador económico cuando la propia persona perjudicada (o una persona de la que aquella sea responsable) haya contribuido por negligencia a la causa de los daños (art. 13.2). Habrá que valorar, en el supuesto concreto, si el producto era defectuoso, pero la persona perjudicada contribuyó a la producción del daño, o si este se ocasionó exclusivamente por su actuación negligente. En este último caso, si resulta acreditada la ruptura total del nexo causal entre el defecto y el daño, de modo que éste no pueda ser atribuido al carácter defectuoso del producto, el operador económico podrá quedar exonerado de responsabilidad⁶¹. Pensemos, por ejemplo, en un supuesto en el que la persona que utiliza el sistema de IA no instale por negligencia actualizaciones que eran necesarias para mantener su nivel adecuado de seguridad, pese a la información proporcionada en las instrucciones de uso⁶², y debido ello se produjeran los daños.

La RLPEPDRPD se ocupa, asimismo, de los supuestos en los que dos o más operadores económicos son responsables de los mismos daños causados a la persona perjudicada (por ejemplo, cuando un componente defectuoso esté integrado en un producto que cause daños). En estos casos, la persona perjudicada puede reclamar una indemnización por los mismos daños tanto al fabricante que integró el componente defectuoso en su producto como al fa-

⁶⁰ La RLPEPDRPD no se pronuncia sobre los casos en los que el daño sea causado exclusivamente por un tercero. La aplicación de las reglas generales de la responsabilidad civil llevaría a justificar la exoneración del operador económico cuando la actuación del tercero fuese de tal entidad, que interrumpiera el nexo de causalidad entre el daño y el defecto del producto. Véase Parra Lucán, MA. “Artículo 133”, en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentario del texto...*, ob. cit., 2015, p. 1926.

⁶¹ Cuando la actuación negligente de la víctima o de una persona de la que aquella deba responder concurra a la producción del daño con el carácter defectuoso del producto, la responsabilidad del operador económico se reducirá. Sin embargo, cuando dicha actuación negligente de la víctima o de una persona de la que aquella deba responder sea la causa única y exclusiva del daño, quedará fundamentada la exoneración de la responsabilidad del operador económico.

⁶² Precisamente, entre la información que ha de incluirse en las instrucciones de uso, figurará las medidas de mantenimiento y cuidado necesarias (incluida su frecuencia) para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a las actualizaciones del *software* (art. 13.3.e del RIA). La previsión y el planteamiento de actualizaciones, -que puede estar en fases anteriores, en concreto, desde el diseño del producto-, no debe centrarse exclusivamente en los nuevos datos y funcionalidades, sino que debe incluir también cómo acceder a ellas. Así, “un producto digital será seguro, no sólo cuando el producto en sí sea seguro, sino, también, cuando sus actualizaciones también lo sean”. Marín Salmerón, A. *El defecto de diseño en los productos digitales*, Aranzadi, Cizur Menor, 2023, pp. 59 y 60.

bricante del propio componente defectuoso (art. 12.1 de la RLPEPDRPD)⁶³. Así, en estas situaciones, para garantizar la protección de las personas físicas, todas las partes deben ser consideradas responsables solidariamente. Se prevé en estos supuestos, con arreglo a lo establecido en el Derecho nacional, la posibilidad de ejercer el derecho de repetición⁶⁴. En la RLPEPDRPD se prevé que el fabricante que incorpore el componente de programa informático defectuoso en su producto, pueda acordar contractualmente con el fabricante de dicho componente (tratándose de una microempresa o una empresa pequeña) renunciar al ejercicio de dicho derecho de repetición⁶⁵.

Las expectativas de seguridad del producto han de valorarse también en relación con el momento en que el producto fue introducido en el mercado o puesto en servicio. Si después de ese momento el fabricante sigue conservando el control sobre el producto, habrá de considerarse también el momento en que el producto dejó de estar bajo su control (art. 7.2.e de la RLPEPDRPD)⁶⁶. Los sistemas de IA están sujetos a posibles cambios y modificaciones. Es posible que determinadas deficiencias del producto tengan lugar después de que el sistema de IA se introduzca en el mercado o se ponga en servicio. La cuestión es si esto determina que el fabricante sea el responsable de los daños derivados de aquellas deficiencias. La cuestión clave para responder a este interrogante es si estas se producen como resultado de programas

⁶³ Según dispone el artículo 12.1 de la RLPEPDRPD: «sin perjuicio de las disposiciones nacionales en relación con los derechos de división de la responsabilidad o de repetición, los Estados miembros garantizarán que, cuando dos o más operadores económicos sean responsables de los mismos daños con arreglo a la presente Directiva, puedan ser considerados responsables solidariamente».

⁶⁴ El artículo 14 de la RLPEPDRPD señala, en relación con este derecho, lo siguiente: «Cuando más de un operador económico sea responsable de los mismos daños, un operador económico que haya indemnizado a la persona perjudicada tendrá derecho a reclamar de otros operadores económicos responsables de conformidad con lo dispuesto en el artículo 8 y en virtud del Derecho nacional». El fabricante del componente podrá eximirse de responsabilidad cuando demuestre que el carácter defectuoso del producto al que se ha incorporado el componente es imputable al diseño del producto o a las instrucciones que le ha dado el fabricante del producto (art. 11.1.f).

⁶⁵ Véase art. 12. 2 de la RLPEPDRPD. Entre las principales razones que justifican esta disposición está la de apoyar la capacidad innovadora de las microempresas y las pequeñas empresas que fabrican programas informáticos. Como señala el considerando 54, se les debe ofrecer a estas la posibilidad de acordar contractualmente con los fabricantes que incorporen a los productos sus programas informáticos que estos últimos no ejercitarán su derecho de repetición frente a ellos en caso de que un componente de software defectuoso cause daños. «Dichos acuerdos contractuales, que ya se utilizan en algunos Estados miembros, deben permitirse, ya que el fabricante del producto en su conjunto es responsable, en cualquier caso, de todo posible carácter defectuoso del producto, también de los componentes. Sin embargo, la responsabilidad frente a una persona perjudicada nunca debe quedar limitada o excluida por un acuerdo contractual de ese tipo» (considerando 54).

⁶⁶ Como señala el considerando 32 de la RLPEPDRPD: «Para reflejar el hecho de que, en la era digital, muchos productos permanecen bajo el control del fabricante tras su introducción en el mercado, el momento en que el producto deja de estar bajo el control del fabricante también debe tenerse en cuenta en la valoración de su seguridad».

informáticos o servicios conexos que estén «bajo su control», ya sea en forma de actualizaciones o mejoras o de algoritmos de aprendizaje automático.

Antes de responder a esta cuestión es preciso aclarar los siguientes conceptos: el «servicio conexo» es definido como: «un *servicio digital* que está *integrado* en un producto o *interconectado* con él, de tal manera que *su ausencia impediría al producto realizar una o varias de sus funciones*» (art. 4.3 RLPEPDRPD) (el subrayado es nuestro). Los servicios conexos deben considerarse como *componentes* del producto en el que están *integrados* o al que están *interconectados cuando están bajo el control del fabricante de dicho producto*. El «componente» es definido como: «cualquier artículo, ya sea *tangible* o *intangible*, materia prima o *servicio conexo*, que está *integrado* en un producto o *interconectado* con él» (art. 4.4.) (el subrayado es nuestro)⁶⁷.

Supongamos que el fabricante de un sistema de IA que sirve de soporte al profesional médico para diagnosticar el cáncer de mama autoriza la actualización del software a la luz de los últimos avances en aprendizaje profundo que permiten analizar mamografías de forma más exhaustiva, identificando anomalías en tejidos mamarios más densos. Si hay una deficiencia en el sistema de IA debido a dicha actualización y se producen daños, una de las cuestiones a valorar será si fue el propio fabricante quien realizó dicha actualización o fue un tercero quien la suministró bajo su autorización. Pues, en este caso, sería posible interponer la reclamación de indemnización, (sin descartar la posible responsabilidad de otros sujetos involucrados)⁶⁸, frente al fabricante del

⁶⁷ Como ejemplos de servicios conexos, el considerando 17 señala los siguientes: «el suministro continuo de datos de tráfico en un sistema de navegación, el servicio de vigilancia de la salud que se basa en sensores de un producto físico para rastrear la actividad física o los parámetros de salud del usuario, el servicio de control de la temperatura que monitoriza y regula la temperatura de un frigorífico inteligente, o un servicio de asistente de voz que permite controlar uno o más productos utilizando comandos de voz». Según hemos señalado, la información no debe considerarse un producto. La cuestión es ¿qué consideración merecen los datos? Pues estos desempeñan un papel esencial a la hora de proporcionar una estructura y garantizar el funcionamiento de muchos sistemas de IA; en especial, cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA funcione del modo previsto y en condiciones de seguridad. Consideramos que, con independencia de que los datos se suministren de manera puntual o periódicamente, lo relevante, para incluirlos en la noción de componente, es que resulten necesarios para el funcionamiento del sistema de IA y se suministren bajo el control del fabricante. Esto es, que dichos datos formen parte de este para el desempeño de sus funciones o reflejen estas en sus resultados de salida generados, tales como predicciones, contenidos, recomendaciones o decisiones. Los conjuntos de datos utilizados condicionan la seguridad del sistema y pueden, en su caso, motivar su carácter defectuoso. Como hemos señalado, deben instaurarse prácticas adecuadas de gestión y gobernanza de datos con el fin de lograr que los conjuntos de datos utilizados, por ejemplo, para el entrenamiento y validación del sistema, sean de alta calidad, representativos, completos y libres de errores en vista a la finalidad prevista de dicho sistema de IA.

⁶⁸ En el caso de que el sistema de IA no mostrase el tumor (debido, por ejemplo, a una actualización del software de procesamiento de imágenes médicas o un mal funcionamiento de este) o lo

sistema de IA, al efectuarse dicha actualización *bajo su control* (art. 11.2.b de la RLPEPDRPD)⁶⁹.

Por tanto, es preciso extender, como hace la RLPEPDRPD, la responsabilidad del fabricante a momentos posteriores al de la introducción en el mercado o puesta en servicio, siempre que siga ejerciendo un control sobre el producto⁷⁰. Como señala el considerando 19: «una vez que un producto se haya introducido en el mercado, debe considerarse que permanece bajo el control del fabricante siempre que este conserve la capacidad de suministrar actualizaciones o mejoras de los programas informáticos bien por sí mismo, bien por medio de terceros».

El fabricante también se considerará responsable cuando se produzca una modificación sustancial del producto bajo su control. Sin embargo, si una persona (física o jurídica) modifica sustancialmente un producto fuera del control del fabricante y, posteriormente, lo comercializa o pone en servicio, se considerará fabricante del producto a efectos del apartado 1, artículo 8 de la RLPEPDRPD. Esto es, cuando dicha modificación se realice en un producto, fuera del control del fabricante original, se considerará un producto nuevo y es posible responsabilizar a la persona que efectuó la modificación sustancial como fabricante de dicho producto modificado. Dicha persona es responsable de que el producto cumpla con los respectivos requisitos de seguridad.

calificase incorrectamente como no maligno (debido a que los datos y modelos en los que se basó el software fueron incompletos), etc., la responsabilidad del profesional médico dependerá, entre otros factores, de la posibilidad de reconocer el error y de su negligencia al actuar (por ejemplo, por no haber constatado y/o contrastado la indicación dada por el sistema de IA a la luz de las circunstancias particulares presentadas por el paciente y/o por no haber realizado, en su caso, pruebas diagnósticas de otra naturaleza que le hubieren llevado a corroborar que la indicación dada por el sistema de IA era incorrecta, de conformidad, por ejemplo, con el estado actual de la ciencia médica.

⁶⁹ Según dispone el artículo 11.2, «un operador económico no estará exento de responsabilidad cuando el defecto de un producto se deba a alguna de las causas siguientes, siempre que esté bajo el control del fabricante: a) un servicio conexo; b) *programas informáticos, incluidas las actualizaciones o mejoras de programas informáticos*» (el subrayado es nuestro). El «control del fabricante» es definido en los siguientes términos: «a) la acción del fabricante de un producto mediante la que realiza o, con respecto a las acciones de un tercero, autoriza o consiente en: i) la integración, interconexión o suministro de un componente, incluidas las actualizaciones o mejoras de los programas informáticos, o ii) la modificación del producto, incluidas las modificaciones sustanciales; b) la capacidad del fabricante de un producto de suministrar actualizaciones o mejoras de programas informáticos, por sí mismo o a través de un tercero (art. 4.5 de la RLPEPDRPD).

⁷⁰ Como señala el considerando 18 de la RLPEPDRPD: «Los servicios conexos y otros componentes, incluidas las actualizaciones y mejoras de programas informáticos, deben considerarse bajo el control del fabricante cuando estén integrados en un producto o interconectados con él, o suministrados por el fabricante, o cuando el fabricante autorice o consienta su integración, interconexión o suministro por parte de un tercero (...) o cuando un fabricante presente un servicio conexo o componente como parte del producto aunque sea suministrado por un tercero. No debe considerarse que un fabricante haya dado su consentimiento a la integración o interconexión, por recomendar determinadas marcas o por no prohibir posibles servicios conexos o componentes».

Supongamos, en este sentido, que un sistema de IA destinado a detectar una enfermedad en la población adulta se modificara para ampliar la detección a la población pediátrica; o un sistema de IA destinado a detectar un tipo de cáncer se modificara para ampliar la detección a otro tipo de cáncer⁷¹. La cuestión es cuándo estamos ante una modificación sustancial. El carácter sustancial de una modificación debe determinarse de acuerdo con los criterios establecidos en el Derecho de la Unión y nacional aplicable en materia de seguridad de los productos⁷². En el RIA se señala que, en consonancia con el concepto establecido de «modificación sustancial» de los productos regulados por los actos legislativos de armonización de la Unión, conviene que, cada vez que se produzca un cambio que pueda afectar al cumplimiento del RIA por parte del sistema de IA de alto riesgo (por ejemplo, un cambio de sistema operativo o de arquitectura de software) o cuando cambie la finalidad prevista del sistema, este se considere un sistema de IA nuevo que debe someterse a una nueva evaluación de la conformidad⁷³.

Por tanto, cuando el fabricante original efectúe una modificación sustancial de un sistema de IA utilizado para el diagnóstico, o esta se efectúe bajo su control, y dicha modificación sustancial haga que el sistema de IA sea defectuoso, dicho fabricante no podrá exonerarse de responsabilidad alegando que el carácter defectuoso se originó después de la introducción del sistema de IA en el mercado o de su puesta en servicio (art. 11.2.d). Si es otra persona la que efectuó dicha modificación sustancial, fuera del control del fabricante

⁷¹ Véase Navas Navarro, S., *Daños ocasionados...*, ob. cit., 2022, p. 95. En general, las modificaciones que cambian las funciones originales previstas o que afectan al cumplimiento del producto de los requisitos de seguridad aplicables o modifiquen su perfil de riesgo deben considerarse modificaciones sustanciales (considerando 39 de la RLPEPDRPD).

⁷² En el RIA la «modificación sustancial» es definida como: «un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectado el cumplimiento por parte del sistema de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate». Entre los requisitos obligatorios que debe cumplir un sistema de IA de alto riesgo está la «conservación de registros» (art. 12). Precisamente, entre los acontecimientos que son objeto de registro está: la detección de situaciones que puedan dar lugar a una modificación sustancial. En caso de modificación sustancial de un sistema de IA de alto riesgo, este ha de someterse a un nuevo proceso de evaluación de la conformidad, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue actual (art. 43.4).

⁷³ Véase considerando 128 del RIA. Sin embargo, según añade este considerando, los cambios que se produzcan en el algoritmo y en el funcionamiento de los sistemas de IA que sigan «aprendiendo» después de su introducción en el mercado o su puesta en servicio, a saber, adaptando automáticamente el modo en que desempeñan sus funciones, no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido predeterminados por el proveedor y se hayan evaluado en el momento de la evaluación de la conformidad».

original, es posible responsabilizar a esta como fabricante del producto modificado (art. 8.2 de la RLPEPDRPD). A las modificaciones sustanciales efectuadas mediante una actualización o mejora de programas informáticos se les aplica los mismos principios que las realizadas de otras maneras. Así, cuando una modificación sustancial se realice a través de una actualización o mejora de un programa informático, o por el aprendizaje continuo de un sistema de IA, debe considerarse que el producto sustancialmente modificado se comercializa o pone en servicio en el momento en que se realice efectivamente dicha modificación. La persona que realice esta modificación sustancial podrá exonerarse de responsabilidad en el caso de que demuestre que el daño está relacionado con una parte del producto no afectada por la modificación (art. 11.1.g RLPEPDRPD).

Tampoco podrá el operador económico eximirse de responsabilidad cuando el defecto del producto se deba a una falta de actualizaciones o mejoras de los programas informáticos necesarias para hacer frente a vulnerabilidades de ciberseguridad y/o para mantener la seguridad del producto, siempre que esté bajo su control (art. 11.2.c de la RLPEPDRPD). Asimismo, en reconocimiento de las responsabilidades de los fabricantes en virtud del Derecho de la Unión en materia de seguridad de los productos a lo largo de todo su ciclo de vida, (como en el Reglamento (UE) 2017/745), se señala en el considerando 51 que: «tampoco debe eximirse de responsabilidad a los fabricantes por los daños causados por sus productos defectuosos cuando el carácter defectuoso sea consecuencia de su falta de suministro de actualizaciones o mejoras de la seguridad de los programas informáticos que sean necesarias para hacer frente a las vulnerabilidades de los productos en respuesta a la evolución de los riesgos de ciberseguridad»⁷⁴.

Asimismo, entre las nuevas circunstancias que se contemplan en la RLPEPDRPD para la valoración de la seguridad de un producto, están las siguientes: «el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio» (art. 7.2.c); así como: «el efecto razonablemente previsible en el producto de otros productos de los que se pueda esperar que se utilicen junto con el producto, también mediante interconexión» (art. 7.2.d). La inclusión de estas circunstancias resulta esencial, dadas las características específicas que describen a muchas tecnologías digitales. El programa informático de un producto y los algoritmos subyacentes han de diseñarse de tal manera

⁷⁴ La responsabilidad no será imputable al fabricante del producto cuando, como hemos señalado, el suministro o la instalación de los programas informáticos escapen del control del fabricante (por ejemplo, porque el propietario del producto no instale una actualización o mejora suministrada para garantizar el nivel de seguridad del producto) (considerando 51).

que se eviten comportamientos peligrosos del producto. Habrá que valorar la posibilidad de que el fabricante que diseñe un producto con la capacidad de desarrollar acciones inesperadas siga siendo responsable, en su caso, de aquellas que causen los daños⁷⁵.

Por otra parte, con el fin de reflejar la importancia de la legislación sobre seguridad de los productos y vigilancia del mercado para evaluar y determinar el nivel de seguridad que el público en general tiene derecho a esperar, debe tenerse en cuenta en la valoración del carácter defectuoso de un producto: «los requisitos de seguridad [de este], incluidos los requisitos de ciberseguridad pertinentes para la seguridad» (art. 7.2 f de la RLPEPDRPD)⁷⁶, y «cualquier retirada del producto o cualquier intervención pertinente de una autoridad competente o de un operador económico (...) en relación con la seguridad de los productos» (art. 7.2. g de la RLPEPDRPD). Sin embargo, dichas intervenciones no deben crear por sí solas una presunción del carácter defectuoso del producto⁷⁷.

⁷⁵ Esta circunstancia ha sido examinada en la doctrina para valorar la seguridad del producto. Así, se considera que, si el diseño de un producto incluye la posibilidad de que este adquiriera nuevas características o las cambie en el futuro, dicha posibilidad es relevante para valorar su seguridad. Se parte de la idea de que, si el diseño del producto incluye la posibilidad de que, una vez introducido en el mercado o puesto en servicio, este adquiriera características peligrosas, dicho producto pueda considerarse, en su caso, defectuoso. Véase European Law Institute, *Draft of a Revised Product Liability Directive. Draft Legislative Proposal of the European Law Institute*, 2022, p. 20; Herrera de la Heras, R., *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022, p. 97. Hay quienes se preguntan si la capacidad de autoaprendizaje y, por ende, la imprevisibilidad/impredecibilidad del comportamiento de estas nuevas tecnologías las convierten en inseguras y por ello en defectuosas. “¿El autoaprendizaje significa, por sí mismo, que el sistema tiene propiedades peligrosas?; ¿O se considerará defectuoso cuando, fruto del aprendizaje, adopte soluciones erróneas?”. Véase Atienza Navarro, ML., op. cit., 2023, p. 17. En cuanto a los sistemas que tienen la capacidad de autoaprendizaje, el operador económico no debe poder eludir la responsabilidad alegando que el daño fue causado por un sistema de IA cuyas características y capacidades podían conllevar a un comportamiento imprevisible potencialmente peligroso. Esto se deriva de conceptos de justicia en materia de responsabilidad civil ampliamente aceptados y de carácter general. En virtud de estos la persona que crea o mantiene un riesgo para el público es responsable si dicho riesgo causa un daño o un perjuicio y, por tanto, debe minimizar *ex ante* (cumpliendo con los respectivos requisitos de seguridad) o indemnizar *ex post* dicho riesgo; en este caso, si se materializa en daño. En cuanto a los cambios que puedan producirse en el algoritmo y en el funcionamiento de los sistemas de IA que sigan aprendiendo después de su introducción en el mercado o puesta en servicio, el RIA contempla la posibilidad de que estos hayan sido, en su caso, predeterminados por el proveedor y evaluados en el momento de la evaluación de la conformidad.

⁷⁶ Véase el art. 15 del RIA, referente al requisito obligatorio de diseñar y desarrollar un sistema de IA de alto riesgo de modo que alcance un nivel adecuado de precisión, solidez y ciberseguridad y funcione de manera uniforme en esos sentidos durante todo su ciclo de vida. Véase, asimismo, los considerandos 74, 75, 76, 77 y 78.

⁷⁷ No debe olvidarse, por otra parte, que el cumplimiento de la correspondiente normativa de seguridad no excluye que el producto pueda provocar daños y pueda ser defectuoso. Como ha seña-

Asimismo, se incluyen entre las circunstancias para valorar la seguridad de los productos: «las necesidades específicas del grupo de usuarios finales a los que se destina el producto» (art. 7.2.h de la RLPEPDRPD)⁷⁸. Y, también, «en el caso de un producto cuya finalidad es precisamente evitar daños, el eventual incumplimiento de dicha finalidad por parte del producto» (art. 7.2.i de la RLPEPDRPD). Por ejemplo, «un mecanismo de alerta como un detector de humos, la valoración del carácter defectuoso de tal producto debe tener en cuenta que no haya cumplido dicha finalidad» (considerando 33).

Por último, hay que tener en cuenta que la posterior introducción en el mercado o puesta en servicio de un producto mejor, incluidas las actualizaciones o mejoras de un producto, no debe llevar por sí a la conclusión de que un producto es defectuoso o que el suministro de dichas actualizaciones o mejoras permitan considerar que una versión anterior del producto era defectuosa (Art. 7.3 de la RLPEPDRPD). Algo que, en general, será habitual en productos que dependen de elementos digitales para funcionar. Pues, dichos productos pueden estar sujetos, como hemos señalado, a actualizaciones periódicas, ya sea para mejorar su funcionalidad, corregir errores o solucionar problemas de seguridad. Se trata, asimismo, de fomentar la investigación e innovación de estos productos que están en constante evolución.

En suma, el cumplimiento de la correspondiente normativa de seguridad aplicable al sistema de IA utilizado para el diagnóstico, servirá como punto de referencia y criterio que, entre otros, contribuye a dar forma a las expectativas de seguridad que cabe legítimamente esperar por el público en general, así como por los profesionales médicos que vayan a utilizarlo como herramienta en la práctica médica. Sin olvidar, no obstante, que el cumplimiento de dicha normativa no excluye el hecho de que dicho sistema de IA pueda ser defectuoso y ocasionar daños. Ambas normativas, la seguridad del producto y la responsabilidad del producto son mecanismos complementa-

lado la jurisprudencia en relación con esta materia, el cumplimiento de la normativa de seguridad no determina necesariamente la ausencia de responsabilidad del fabricante. Véase, entre otras, la STS de 10 de junio de 2002 (RJ 2002/6198); SAP de Valencia de 12 de julio de 2001 (JUR 2001/279709).

⁷⁸ Las expectativas de seguridad serán más altas, por ejemplo, para sistemas de IA utilizados, entre otras finalidades, para el triaje de pacientes en aras de recibir la asistencia en emergencias. El desvío en la predicción clínica sobre la urgencia puede causar graves daños al paciente. Piénsese también en dispositivos quirúrgicos cuyo fallo pone en riesgo la vida de las personas. La comercialización de estos productos no se debe producir hasta haber superado los umbrales de seguridad legalmente establecidos, que serán tan altos como elevados son los bienes jurídicos que pueden verse afectados por dichos sistemas de IA. En el considerando 30 de la RLPEPDRPD, en virtud de esta línea de argumentación, se señala que: «algunos productos, como los productos sanitarios de soporte vital, conllevan un riesgo especialmente elevado de daños para las personas y, por lo tanto, generan unas expectativas de seguridad especialmente elevadas. Para tener en cuenta estas expectativas, el órgano jurisdiccional debe poder considerar defectuoso un producto sin que se declare probado su verdadero carácter defectuoso, cuando pertenezca a la misma serie de producción que un producto cuyo carácter defectuoso ya ha sido probado».

rios, (uno situado en el plano de la prevención de los riesgos, el otro situado en la reparación, una vez que los riesgos se materializan en daños). Si bien, ambos mecanismos complementarios tienen como objetivo básico lograr un mercado de bienes único y operativo que garantice niveles elevados de seguridad.

Este régimen de responsabilidad por producto defectuoso es de carácter objetivo y prescinde de la culpa como criterio de imputación. Si bien, con el fin de lograr un reparto equitativo del riesgo, una persona que reclame una indemnización por los daños causados por un producto defectuoso, (el paciente que ha sufrido daños como consecuencia de una decisión médica basada en una indicación errónea dada por el sistema de IA, que no ha funcionado correctamente)⁷⁹, debe soportar la carga de la prueba del daño, el carácter defectuoso del producto y el nexo de causalidad entre ambos, de conformidad con el nivel de prueba aplicable a la luz del Derecho nacional. La cuestión es cómo impedir que la carga probatoria pueda convertirse en una «*probatio diabolica*», sobre todo, tratándose de un complejo sistema de IA. Pues, con frecuencia, la persona que reclame una indemnización por daños se encontrará en una desventaja significativa frente a los operadores en cuanto al acceso a la información sobre cómo se ha diseñado un sistema de IA y cómo funciona, y en cuanto a la comprensión de esta información. Dicha asimetría de información puede socavar el reparto equitativo del riesgo; en particular, cuando se trata de supuestos de gran complejidad técnica o científica. Esto ha llevado a formular ciertas medidas dirigidas a facilitar el acceso del demandante a las pruebas que vayan a utilizarse en los procesos judiciales y a aligerar la carga de la prueba que le corresponde cuando se cumplan determinadas condiciones.

⁷⁹ El paciente, en este caso, está legitimado activamente para demandar al fabricante. El art. 5 de la RLPEPDRPD dispone que: «Los Estados miembros garantizarán que toda *persona física* que sufra daños causados por un producto defectuoso («la persona perjudicada») tenga derecho a una indemnización de conformidad con la presente Directiva». Como señalan varios autores, el término «persona perjudicada», es cualquier persona física que sufra esos daños como consecuencia de los defectos de los productos fabricados o suministrados por los empresarios; esto es, cualquier ciudadano, tanto el que sea adquirente, como el que utilice o disfrute el producto, así como el que no lo adquiera ni lo disfrute o utilice (bystander). Véase Bercovitz, R. «Artículo 3», en *Comentario del Texto Refundido de la Ley General para la defensa de los Consumidores y Usuarios y otras leyes complementarias*, Bercovitz, R., (Coord.), Aranzadi-Thomson Reuters, Cizur Menor, 2009, pp. 87-91. El bystander es aquel que sin haber usado o consumido directamente el producto sufre accidentalmente las consecuencias dañosas. Véase, también, Camacho Clavijo, S. *La telemedicina. Una aproximación a los distintos modelos de regulación en el marco europeo*, Madrid, Reus, 2024, p. 189. Esta autora considera que la utilización de sistemas de IA en el que «el perjudicado por su funcionamiento puede ser una persona física no adquirente, hará más patente si cabe, una cuestión ya evidenciada por el Reglamento de Roma II, como es la supresión de la obsoleta distinción entre compradores del producto y otras personas perjudicadas».

5. SISTEMA DE EXHIBICIÓN DE PRUEBAS Y CARGA DE LA PRUEBA

El artículo 9 de la RLPEPDRPD prevé un sistema de exhibición de pruebas. En su apartado primero establece que, a petición de la persona que reclame una indemnización en un procedimiento ante un órgano jurisdiccional nacional por los daños causados por un producto defectuoso (demandante), -pretensión cuyo fundamento fáctico y jurídico habrá de acreditar suficientemente-, se exigirá al demandado que exhiba las pruebas pertinentes de que disponga, con arreglo a las condiciones establecidas en el artículo 9. Los apartados 3, 4 y 5 del citado precepto, hacen referencia a la verificación por parte del órgano judicial de que la exhibición de pruebas se limite a lo que resulte necesario y proporcionado⁸⁰. El órgano judicial deberá tener en cuenta los intereses legítimos de todas las personas afectadas, incluidos terceros; en particular, con respecto a la protección de la información confidencial y los secretos comerciales⁸¹. Asimismo, el demandado tiene la posibilidad de obtener pruebas en poder del actor, estableciéndose un equilibrio entre ambas posiciones procesales (art. 9.2)⁸².

Por otra parte, dada la complejidad de determinados tipos de pruebas, (por ejemplo, las relativas a un producto sanitario innovador que es un sistema de IA de alto riesgo), el órgano judicial podrá exigir que dichas pruebas se presenten de forma fácilmente accesible y comprensible, siempre que se cumplan deter-

⁸⁰ Dichas pruebas incluyen los documentos que el demandado deba crear *ex novo* mediante la compilación o clasificación de las pruebas disponibles. El órgano judicial, al examinar la solicitud de exhibición de pruebas, debe garantizar que ese acceso se limite a lo necesario y proporcionado. De este modo, se pretende evitar búsquedas indiscriminadas de información que no sea pertinente para el procedimiento y para proteger información confidencial, como la información que entra en el ámbito del secreto profesional y los secretos comerciales de conformidad con el Derecho de la Unión y nacional (considerando 42).

⁸¹ Como señala el art. 9.5 de la RLPEPDRPD: «Los Estados miembros garantizarán que, cuando se exija a un demandado revelar información que sea un secreto comercial o un supuesto secreto comercial, los órganos jurisdiccionales nacionales estén facultados, previa solicitud debidamente motivada de una parte o por propia iniciativa, para adoptar las medidas específicas necesarias para preservar la confidencialidad de esa información cuando se utilice o se mencione en el transcurso del procedimiento judicial o después de este». Como señala el considerando 45, al decidir sobre tales medidas, es preciso que el órgano judicial tenga en cuenta la necesidad de garantizar la tutela judicial efectiva y a un juez imparcial, los intereses legítimos de las partes y, en su caso, de terceros, así como el perjuicio que pudiera ocasionarse a cualquiera de las partes en el litigio o, en su caso, a terceros, como resultado de que se acuerden o no dichas medidas. En dicho considerando 45 se señalan, por ejemplo, como medidas para garantizar la confidencialidad de los secretos comerciales, las siguientes: restringir el acceso a los documentos que contengan secretos comerciales o presuntos secretos comerciales; restringir el acceso a las audiencias a un número limitado de personas, etc.

⁸² Es posible que el demandado pueda necesitar acceder a las pruebas a disposición del demandante para oponerse a una demanda de indemnización. En este sentido, el demandado también tiene la posibilidad de acceder a las pruebas. En este caso, el órgano judicial ha de garantizar, asimismo, que dicho acceso, por las razones ya expuestas, se limite a lo necesario y proporcionado (considerando 44).

minadas condiciones. Así, cuando a una parte se exija la exhibición de pruebas, el órgano judicial estará facultado, (previa solicitud debidamente motivada de la parte contraria o cuando aquel lo estime apropiado y con arreglo al Derecho nacional), para requerir que dichas pruebas se aporten de manera fácilmente accesible y comprensible, cuando dicha aportación, a su juicio, sea proporcionada en términos de costes y esfuerzo para la parte requerida (art. 9.6).

Asimismo, se prevé en la RLPEPDRPD una serie de presunciones dirigidas a aligerar las dificultades probatorias del demandante, permitiendo al órgano judicial basar la existencia de un defecto o de un nexo causal entre el defecto y el daño, en la presencia de otro hecho probado, preservando, a su vez, los derechos del demandado.

En cuanto a las presunciones relativas al carácter defectuoso del producto, se prevé en el artículo 10.2 de la RLPEPDRPD tres condiciones alternativas, de modo que al demandante le bastará alegar y acreditar una de ellas para beneficiarse de la presunción.

Así, con el fin de incentivar el cumplimiento de la obligación de revelar información, el órgano judicial presumirá el carácter defectuoso del producto cuando el demandado incumpla dicha obligación de exhibir las pruebas pertinentes (art. 10.2.a).

Por otra parte, con el fin de reforzar la estrecha relación existente entre las normas de seguridad de los productos y las normas de responsabilidad, se prevé, en el artículo 10.2.b, la posibilidad de presumir el carácter defectuoso del producto cuando se acredite el incumplimiento de los requisitos obligatorios de seguridad establecidos en el Derecho de la Unión o en el Derecho nacional; en concreto, de aquellos requisitos que tengan por objeto proteger contra el riesgo del daño sufrido por la persona perjudicada. La facilidad probatoria radica en que, acreditado el incumplimiento de un requisito de seguridad cuya finalidad sea esta, el órgano judicial considerará que el producto es defectuoso, en el sentido ya señalado; esto es, por no ofrecer el producto la seguridad que una persona tiene derecho a esperar, teniendo en cuenta todas las circunstancias, incluidas las mencionadas en el artículo 7 de la RLPEPDRPD. El demandante tendría que probar, -tratándose, por ejemplo, de un sistema de IA que se usa para el diagnóstico basado en imagen médica-, que determinado o determinados requisitos de seguridad obligatorios se han incumplido a la luz de la normativa aplicable dada su consideración como producto sanitario (por ejemplo, de clase IIa), y como sistema de IA de alto riesgo. El incumplimiento de dichos requisitos daría lugar a una presunción del carácter defectuoso del producto, al tener estos por objeto la protección contra el riesgo del daño sufrido por la persona perjudicada. . El considerando 46 de la RLPEPDRPD señala que el incumplimiento de dichos requisitos

debe dar lugar a una presunción de carácter defectuoso. Indica como ejemplo los casos en que un producto no esté equipado con los medios para registrar información sobre su funcionamiento (tal como, en nuestro caso, exige el RIA en su artículo 12).

Pensemos, por ejemplo, en un sistema de IA utilizado para el diagnóstico de una patología. Puede ocurrir que esta no aparezca en la imagen debido a un mal funcionamiento del software de procesamiento de imágenes, o ser erróneamente clasificada dados los datos o los parámetros con los que ha sido entrenado el sistema de IA, o debido a que estos datos no presentaban los patrones que caracterizaban a dicha patología concreta, etc. Podría suceder, en este caso, que no se hubiese cumplido correctamente con alguno de los requisitos relacionados con la obligación de diseñar el sistema con el nivel adecuado de precisión y solidez y/o con el requisito de desarrollarlo a partir de conjuntos de datos que cumplan los respectivos criterios de calidad. Puede suceder también que, por ejemplo, un sistema de IA utilizado, por ejemplo, para detectar la retinopatía diabética (RD) por oftalmólogos, únicamente se evalúe con conjuntos de datos de pacientes procedentes de un hospital. Esto podría suponer que la herramienta esté sesgada y que, aplicada a pacientes procedentes de diferentes hospitales, resultase ser mucho menos eficaz, con los consiguientes daños derivados de ello para estos. Sin perjuicio de las particularidades y complejidades que presentasen estos casos y otros posibles escenarios (en los que, en su caso, podría tener lugar la responsabilidad del profesional médico y/o centro sanitario), es posible que pudiera demostrarse por el paciente perjudicado que el sistema de IA, por ejemplo, no ha contado con prácticas de gobernanza y gestión de datos adecuadas para su finalidad prevista, al no prever, en este último caso, un examen de los posibles sesgos que podían afectar a la salud de los pacientes y, por tanto, no incluir medidas adecuadas para detectarlos, prevenirlos y mitigarlos, y que dicho requisito estaba dirigido, precisamente a evitar el riesgo del daño producido (indicación errónea del sistema de IA, por no haber clasificado correctamente la RD de la persona perjudicada «RD moderada», con el consiguiente retraso en el diagnóstico, en el tratamiento y reduciéndose las posibilidades de curación)⁸³.

⁸³ En la RLPEPDRPD la persona física que sufra daños causados por un producto defectuoso (la persona perjudicada) tendrá derecho a una indemnización de, entre otros, los siguientes tipos de daños: «muerte o lesiones corporales, incluidos los daños para la salud psicológica comprobados médicamente» (art. 6.1.a). Según lo dispuesto en el art. 6.2, el derecho a indemnización con arreglo al art. 5 cubrirá todas las pérdidas materiales derivadas de dichos daños (por ejemplo, gastos funerarios o médicos o pérdida de ingresos). En el art. 6.1.a se señala que quedan incluidos «los daños para la salud psicológica reconocidos médicamente». En el considerando 21 se aclara que: «las lesiones corporales incluyen los daños para la salud psicológica reconocidos y certificados médicamente que afecten al estado general de la víctima y que puedan requerir terapia o tratamiento médico, teniendo en cuenta, entre otras cosas, la Clasificación Internacional de Enfermedades de la Organización

El artículo 10.2.c contempla la presunción que permite derivar el carácter defectuoso del mal funcionamiento evidente del producto durante el uso razonablemente previsible. Como señala el considerando 46, en el caso de un funcionamiento defectuoso manifiesto, como una botella de vidrio que explota durante su uso razonablemente previsible, resulta innecesariamente gravoso exigir al demandante que demuestre la existencia de un defecto cuando las circunstancias son tales que su existencia es indiscutible⁸⁴.

El artículo 10.3 dispone que: «Se presumirá el carácter defectuoso del producto y el daño cuando se haya comprobado que el producto es defectuoso y el daño causado sea de un tipo compatible normalmente con el defecto en cuestión». El uso de términos como «normalmente compatible», conlleva cierta inseguridad jurídica. En base, principalmente, a casos similares, será preciso que dicho daño sea causado generalmente por el carácter defectuoso en cuestión y que no deba, por tanto, exigirse al demandante que demuestre el nexo causal, presumiéndose, en su caso, su existencia.

El artículo 10.4 prevé la posibilidad de presumir el carácter defectuoso y/o de su nexo causal con el daño producido, cuando, -a pesar de la exhibición de pruebas por parte del demandado- resulte excesivamente difícil para el demandante, debido, especialmente, a la complejidad técnica o científica del caso-, demostrar dichos extremos. En este escenario, el demandante ha de demostrar que es probable que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso y el daño, o ambos⁸⁵. Se ha criticado la indeterminación

Mundial de la Salud». En cuanto a los daños morales, como el dolor y el sufrimiento, derivados de los daños previstos en el art. 6.1, serán cubiertos, según el art. 6.2, en la medida en que puedan ser indemnizados con arreglo al Derecho nacional. En nuestro régimen jurídico, el art. 129.1 del TRLGDCU no los menciona. Según lo dispuesto en el segundo párrafo del art. 128 deberán reclamarse con arreglo a las reglas de responsabilidad contractual o extracontractual. En la RLPEPDRPD se prevé en el art. 6.3 que: «Este artículo no afecta al Derecho nacional relativo a las indemnizaciones en virtud de otros regímenes de responsabilidad». Es posible que la persona perjudicada parte de la reclamación la haga al amparo de este régimen de responsabilidad y otra parte con fundamento en las normas generales de responsabilidad (por ejemplo, para la reclamación de daños no cubiertos por aquel régimen sobre productos defectuosos).

⁸⁴ En un torneo de ajedrez en Moscú, un brazo robótico rompió el dedo a un niño de 7 años con el que jugaba. Disponible en: <https://www.marca.com/ajedrez/2022/07/25/62de569c268e3ea73a8b457f.html> “El niño hizo un movimiento, y después de eso tenemos que dar tiempo para que el robot responda, pero el niño se apresuró, el robot lo agarró”. En nuestra normativa, el uso razonablemente previsible comprende el uso al que está destinado un producto de conformidad con la información facilitada por el operador económico y el uso que pueda preverse razonablemente cuando dicho uso pueda derivarse de un comportamiento lícito y fácilmente previsible. Esto entraría dentro de los términos de la valoración de este caso; esto es, el previsible movimiento repentino o rápido que pudiera realizar el niño. Sin perjuicio, de que, en este caso, pudieran entrar a valorarse también, a la luz de nuestra normativa, otras cuestiones, tales como la concurrencia de la conducta negligente de la víctima en la causación del daño.

⁸⁵ Según el art. 10.4: «El órgano jurisdiccional nacional presumirá el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambos, cuando, a pesar de la exhibición

de la que adolecen los términos utilizados, tales como «dificultades excesivas» o «probable» que conllevan a una falta de claridad del estándar probatorio⁸⁶. Esto se justifica con el argumento de que «los fabricantes tienen conocimientos especializados y están mejor informados que la persona perjudicada» (considerando 48 de la RLPEPDRPD). En este sentido, se considera que aquellos se encuentran en una mejor posición a nivel probatorio que las personas perjudicadas. Así, en casos de gran complejidad técnica o científica, se argumenta que: «imponer el nivel de prueba habitual exigido por el Derecho nacional, que a menudo requiere un alto grado de probabilidad, menoscabaría la efectividad del derecho a indemnización» (considerando 48). Por ello, según señala este considerando, «a fin de mantener un reparto equitativo del riesgo, al tiempo que se evita una inversión de la carga de la prueba, debe exigirse al demandante que demuestre, cuando sus dificultades se refieran a la prueba del carácter defectuoso, únicamente que es probable que el producto fuera defectuoso, o, cuando las dificultades del demandante se refieran a la prueba del nexo causal, únicamente que el carácter defectuoso del producto es una causa probable del daño».

La complejidad técnica o científica debe ser determinada por el órgano judicial caso por caso. Tratándose, por ejemplo, de un sistema de IA que se usa para el diagnóstico basado en imagen médica, se podría tener en cuenta, entre otros, los siguientes factores: la naturaleza compleja de la tecnología utilizada, como el aprendizaje profundo; la naturaleza compleja de la información y los datos que debe analizar el demandante, etc. La valoración de las dificultades excesivas también debe ser realizada por el órgano judicial, caso por caso. Como señala el considerando 48, «si bien el demandante debe aportar argumentos para demostrar la existencia de dificultades excesivas, no debe exigirse la prueba de tales dificultades. Por ejemplo, en una demanda relativa a un sistema de IA, para que el órgano jurisdiccional decida que existen dificultades excesivas, no debe exigirse al demandante que explique las características específicas del sistema de IA ni cómo estas características dificultan la determinación del nexo causal».

de pruebas de conformidad con el artículo 9 y teniendo en cuenta todas las circunstancias pertinentes del caso: a) el demandante se enfrente a *dificultades excesivas*, en particular debido a la complejidad técnica o científica para demostrar el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambos, y b) el demandante demuestre que es *probable* que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso del producto y el daño, o ambos» (el subrayado es nuestro).

⁸⁶ Como señala Atienza Navarro, ML., dicha indeterminación suscita varias cuestiones. Por ejemplo, «la exigencia, para que se aplique la presunción, de que sea probable que el producto fue defectuoso o que la defectuosidad fue la causa «probable» del daño, plantea el interrogante de cómo puede probarse que el defecto fue una causa del daño sin probar su carácter defectuoso, y, sobre todo, provoca el inconveniente de cómo valorar esa probabilidad (¿bastaría demostrar un 51% de probabilidad o sería superior?). Véase Atienza Navarro, ML., op. cit., 2023, p. 37. En nuestro caso, tratándose de un sistema de IA que está destinado a proporcionar información de diagnóstico precisa y exacta (es la seguridad que legítimamente cabe esperar del mismo), el hecho de que proporcione información errónea podría llevar a presumir, en su caso, su carácter defectuoso.

En todos estos casos (apartados 2, 3 y 4 del artículo 10) se trata de presunciones *iuris tantum* que, en este sentido, podrá refutar y, en su caso, destruir el demandado a través de la prueba de la inexistencia del defecto y/o del nexo causal entre este y el daño (art. 10.5). «El demandado debe tener la posibilidad de impugnar todos los elementos de la demanda, incluida la existencia de dificultades excesivas» (cdo. 48).

6. CAUSAS DE EXONERACIÓN: ESPECIAL CONSIDERACIÓN A LOS RIESGOS DEL DESARROLLO

Las causas de exoneración están contempladas en el artículo 11 de la RLPEPDRPD. La denominada «exoneración basada en los riesgos del desarrollo» adquiere una importancia especial cuando se trata de productos innovadores basados en IA. Según lo dispuesto en dicho precepto, en el apartado 1, letra e: «Los operadores económicos a que se refiere el artículo 8 no serán responsables de los daños causados por un producto defectuoso si demuestran que: el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso». En el considerando 52, se pone de manifiesto que dicho «estado de los conocimientos científicos y técnicos», viene determinado con referencia «al *nivel más avanzado* de conocimiento *objetivo accesible* y no al conocimiento *efectivo* del operador económico en cuestión» (el subrayado es nuestro). Esta referencia se presta a ciertos problemas interpretativos⁸⁷. En general, es preciso que el nivel más avanzado de los conocimientos y de las investigaciones realizadas hasta un determinado momento⁸⁸, sean accesibles a la

⁸⁷ Por ejemplo, ¿en qué términos se traduce dicha accesibilidad? La cuestión de la accesibilidad tiene gran relevancia en el contexto del desarrollo de la IA. Habrá que valorar, en cada caso concreto, los términos en que se traduce dicha accesibilidad. «¿Debería una PYME de los Países Bajos poder sustentar esta causa de exoneración si el defecto pudiera prevenirse mediante el conocimiento publicado en una pequeña revista científica portuguesa? (...)» Véase, en este sentido, Cabral, TS. “Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive”, *Maastricht Journal of European and Comparative Law*, vol. 27, 5, 2020, pp. 615-635; p. 623. Como afirma este autor la carga de la prueba recae sobre el fabricante. Corresponde a este probar que no existían conocimientos científicos y/o técnicos disponibles en el momento de la puesta en circulación del producto que pudieran haber evitado un defecto.

⁸⁸ Como hemos señalado, los nuevos productos en la era digital permiten que los fabricantes mantengan un control sobre ellos más allá del momento en que se introducen en el mercado, o de su puesta en servicio. Periodo en el que continúa avanzando el estado de los conocimientos científicos y técnicos relevantes para el concreto producto. En este sentido, el nivel más avanzado de conocimiento objetivo accesible entra a valorarse también durante el período en que el producto estaba bajo el control del fabricante.

comunidad científica⁸⁹, y se hallen respaldados por su rigurosidad, autenticidad, etc.

Se argumenta que, con esta causa de exoneración, se permite, en un régimen de responsabilidad objetiva, la entrada de la culpa o negligencia para imputar la responsabilidad al fabricante⁹⁰. Pues, si permitimos a este exonerarse de responsabilidad demostrando que el estado objetivo los conocimientos científicos y técnicos no permitía descubrir el defecto cuando introdujo su producto en el mercado, o cuando lo puso en servicio, o durante el período en que estaba bajo su control, volvemos a incluir aspectos relacionados con la diligencia⁹¹

Se ha mantenido, no obstante, esta causa de exoneración, entre otras razones porque se considera que esta contribuye a conservar el equilibrio entre

⁸⁹ Véase STS (Sala de lo Contencioso-Administrativo, Sección 4ª) Sentencia de 11 junio 2012 (RJ 2012\7330). En esta sentencia se considera que «se dan los requisitos para declarar la responsabilidad patrimonial solicitada por la demandante y ello porque ha existido un error de diagnóstico con vulneración de “la lex artis ad hoc “ya que, aunque la actividad médica no es una actividad de resultado sino de medios, ha quedado acreditado que no se utilizaron todos los medios necesarios (...) que la ciencia médica exigía “entendiendo por tal el estado de los conocimientos científicos y técnicos en el nivel más avanzado de las investigaciones, que comprende todos los datos presentes en circuito informativo de la comunidad científica o técnica en su conjunto...”» (el subrayado es nuestro).

⁹⁰ Se afirma que, mientras subsista esta causa de exoneración, cabe considerar que la responsabilidad que se imputa al fabricante está basada en la diligencia de este (como buen profesional) para averiguar la posible existencia del defecto. Esto resulta discordante en el ámbito de una responsabilidad de corte objetivo. Véase Bercovitz Rodríguez-Cano, R. “La responsabilidad de los fabricantes en la Directiva de las Comunidades Europeas de 25 de junio de 1985”, *Estudios sobre consumo*, núm. 7, 1986, p. 7; Bertolini, A. *Artificial Intelligence and civil liability*, 2020, p. 59. En opinión de otros autores, se considera que la excepción de los riesgos del desarrollo, rectamente entendida, sólo tiene sentido en un sistema de responsabilidad objetiva o sin culpa. Véase, en este sentido, Busto Lago, JM., Álvarez Lata, N., Peña López, F., *Reclamaciones de consumo. Derecho de consumo desde la perspectiva del consumidor*, Thomson Reuters Aranzadi, Cizur Menor, 2010, p. 769.

⁹¹ Desde un sector de la doctrina se propugna la eliminación de esta causa de exoneración en el ámbito de los daños causados por sistemas de IA. Navarro Michel, M. “Vehículos automatizados y responsabilidad por producto defectuoso”, *Revista de Derecho Civil*, núm. 5, 2020, pp. 175-223; p. 215. La autora señala que: “En aras a la protección de las víctimas, y para potenciar la confianza en el nuevo sector de automoción, resultaría aconsejable excluir la posibilidad de alegación de la excepción por riesgos de desarrollo por parte del fabricante de vehículos automatizados”; Gómez Ligüerre, C., y García-Micó TG. “Liability for Artificial Intelligence and other emerging technologies”, *InDret*, 1, 2020, pp. 501-511; p. 509, donde los autores señalan que, en entornos con un alto nivel de innovación, su adopción generalizada “podría liberar de responsabilidad a buena parte de los potenciales responsables. En perjuicio de las víctimas y en beneficio de productores y, acaso también, del progreso mismo de la ciencia”. Casadesus Ripoll, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, *Revista de la facultad de Derecho de México*, núm. 278, 2020, pp. 353-373; p. 367; BEUC (The European Consumer Organization). *Product Liability 2.0 How to make EU rules fit for consumers in the digital age*. Ref: BEUX-X-2020-024. 07/05/2020, pp. 12-13, donde se afirma la necesidad de suprimir esta causa de exoneración, dada la velocidad con la que avanzan las nuevas tecnologías.

la necesidad de promover la introducción en el mercado de productos innovadores y la protección de los consumidores, en la medida en que rebaja el coste de los seguros de las empresas⁹². Si bien, en la RLPEPDRPD se prevé la posibilidad de que los Estados miembros puedan establecer excepciones a esta causa de exoneración. Así, se establece que estos puedan mantener en sus sistemas jurídicos las medidas vigentes que excluyen esta causa de exoneración (art. 18.1)⁹³, introducir nuevas medidas o modificar las vigentes (art. 18.2), ampliando la responsabilidad de los operadores económicos en estas situaciones a categorías específicas de productos. Dichas medidas, además de estar limitadas a tipos específicos de productos (art. 18.3.a), estarán justificadas por objetivos de interés público (art. 18.3.b) y serán proporcionadas, «en el sentido de que serán adecuadas para garantizar la consecución de los objetivos perseguidos y no excederán de lo necesario para alcanzarlos» (art. 18.3.c)⁹⁴.

Nuestro sistema jurídico mantiene esta causa de exoneración de los fabricantes excepto en los casos de medicamentos, alimentos o productos alimentarios destinados al consumo humano⁹⁵. Cuando se trate de este tipo de

⁹² Se afirma que: “la prima del seguro será elevada, precisamente, porque no se sabe si los conocimientos científicos y técnicos podrían descubrir un defecto en el producto”. Marín Salmerón, A. op. cit., 2023, p. 257. Desde esta perspectiva, se defiende que mantener esta causa de exoneración favorece el progreso de la ciencia y la técnica. Pues, puede suceder que “ante el temor de responder por «defectos» que no pudieron ser evitados en el momento de la creación del sistema inteligente, se opte por no arriesgar en la fabricación de nuevas tecnologías”. Véase Atienza Navarro, ML. *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Madrid, 2022, p. 196; NÚÑEZ Zorrilla, MC. *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019, pp. 40-41; Cabral, TS., op. cit., 2020, pp. 623-624. Para alcanzar el equilibrio entre la necesidad de mantener e incentivar la innovación y los intereses de los consumidores, constituye un factor importante esta causa de exoneración relativa al riesgo del desarrollo.

⁹³ En estos casos, se exige que el Estado miembro que desee mantener dichas medidas notifique el texto de estas a la Comisión. Esta informará de ello a los demás Estados miembros (véase art. 18.1 *in fine*).

⁹⁴ «Todo Estado miembro que desee introducir o modificar una medida de conformidad con el apartado 2 notificará el texto de la medida propuesta a la Comisión y justificará de qué manera dicha medida cumple lo dispuesto en el apartado 3. La Comisión informará de ello a los demás Estados miembros» (art. 18.4). A partir de la recepción de una notificación a este respecto, «la Comisión podrá emitir un dictamen sobre el texto de la medida propuesta y su justificación, teniendo en cuenta las observaciones recibidas de otros Estados miembros. El Estado miembro que desee introducir o modificar una medida la dejará en suspenso durante los seis meses siguientes a su notificación a la Comisión, a menos que esta emita su dictamen antes» (art. 18.5).

⁹⁵ Según lo dispuesto en el art. 140.3 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU): «En el caso de medicamentos, alimentos o productos alimentarios destinados al consumo humano, los sujetos responsables, de acuerdo con este capítulo, no podrán invocar la causa de exoneración del apartado 1, letra e)» («riesgos del desarrollo»).

productos, el fabricante no podrá eximirse de responsabilidad alegando esta causa de exoneración.

Resulta esencial que, aunque no se hayan producido daños después de introducirse en el mercado o ponerse en servicio el sistema de IA utilizado para el diagnóstico, el proveedor (en cooperación con otros operadores) cumpla con el respectivo deber de vigilancia y de diligencia en el tráfico, sobre todo en vista de lo rápido que avanzan los conocimientos en materia de IA, en aras de adoptar todos los mecanismos adecuados para prevenir o evitar los posibles daños. Es preciso seguir un sistema de vigilancia poscomercialización⁹⁶. El fabricante debe planificar, establecer, documentar, aplicar, mantener y actualizar este sistema de seguimiento poscomercialización de un modo proporcionado a la clase de riesgo y de forma adecuada al tipo de producto⁹⁷. Se pretende, así, recabar, conservar y analizar los datos pertinentes sobre calidad, funcionamiento y seguridad del producto, durante todo su ciclo de vida, extraer las conclusiones pertinentes y determinar, aplicar y supervisar cualquier actuación preventiva y correctiva⁹⁸. Tratándose de un sistema de IA de alto riesgo regulado por el Reglamento (UE) 2017/745, al estar ya establecido un sistema y un plan de vigilancia poscomercialización con arreglo a este, y a fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los elementos necesarios descritos en los apartados 1, 2 y 3 del artículo 72 del RIA, utilizando el modelo a que se refiere el apartado 3, en los sistemas y planes que ya existan en virtud de lo dispuesto en el Reglamento (UE) 2017/745, siempre que alcance un nivel de protección equivalente (véase art. 72.4 del RIA).

⁹⁶ El «seguimiento poscomercialización» se define como: «todas las actividades realizadas por los fabricantes en cooperación con otros agentes económicos para instaurar y actualizar un procedimiento sistemático destinado a recopilar y examinar de forma proactiva la experiencia obtenida con productos que introducen en el mercado, comercializan o ponen en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctiva o preventiva» (art. 2.60 del Reglamento (UE) 2017/745). Véase, también, la definición de «sistema de vigilancia poscomercialización» recogida en el art. 3.25 del RIA: «todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger y examinar la experiencia obtenida con el uso de sistemas de IA que introducen en el mercado o ponen en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctora o preventiva que resulte necesaria». Este sistema es también fundamental para garantizar que los posibles riesgos derivados de sistemas de IA que siguen «aprendiendo», tras su introducción en el mercado o puesta en servicio, se aborden de una manera eficiente y oportuna.

⁹⁷ Sistema que, como añade el art. 83.1 del Reglamento (UE) 2017/745, será parte integrante del sistema de gestión de calidad del fabricante indicado en el artículo 10, apartado 9.

⁹⁸ Véase art. 83.2 del Reglamento (UE) 2017/745. En el art. 83.3 se señalan los fines para los que, en particular, se destinarán los datos recogidos por dicho sistema de seguimiento poscomercialización (por ejemplo, para detectar necesidades de acciones preventivas, correctivas o de acciones correctivas de seguridad).

Resulta esencial contar con este sistema de vigilancia poscomercialización para, a la luz de la experiencia con el uso del sistema de IA de alto riesgo de que se trate, se pueda mejorar, en su caso, el proceso de diseño y desarrollo o se pueda adoptar las medidas correctoras oportunas⁹⁹. En este contexto, resulta exigible que los proveedores cuenten también con un sistema para comunicar a las autoridades pertinentes cualquier incidente grave asociado al uso de sus sistemas de IA¹⁰⁰. Incidentes que pueden derivar de fallos o defectos que no permitió, en su momento, detectar el estado objetivo de los conocimientos científicos y técnicos¹⁰¹. La notificación ha de efectuarse «inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave»¹⁰².

En suma, los fabricantes deben desempeñar un papel activo durante esta fase, recabando información sobre la experiencia poscomercialización con sus productos, con el fin de revisar su documentación técnica y de colaborar con las autoridades nacionales competentes encargadas de las actividades de vigilancia y control del mercado. Los datos y la información pertinentes recabados por medio de este sistema de seguimiento, así como las conclusiones derivadas de cualquier acción preventiva y/o correctiva aplicada, deben servir para actualizar la documentación técnica, como la relativa a la evaluación del

⁹⁹ Véase la definición de «acción correctiva de seguridad» del artículo 2.68 del Reglamento (UE) 2017/745: «acción correctiva efectuada por un fabricante por motivos técnicos o médicos para evitar o reducir el riesgo de un incidente grave [definido en el art. 2.65] en relación con un producto comercializado». En el RIA «el incidente grave» se define como: «un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias: a) el fallecimiento de una persona o un perjuicio grave para su salud; b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas; c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales; d) daños graves a la propiedad o al medio ambiente» (art. 3.49).

¹⁰⁰ En el artículo 73.10 del RIA se señala que: «En el caso de los *sistemas de IA de alto riesgo* que sean componentes de seguridad de dispositivos, o que en *sí mismos sean dispositivos*, regulados por los *Reglamento (UE) 2017/745* y (UE) 2017/746, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c), del presente Reglamento, y se hará a la autoridad nacional competente elegida para tal fin por los Estados miembros en los que se haya producido el incidente». El art. 3.49.c del RIA se refiere a aquel incidente o defecto de funcionamiento del sistema de IA que, como consecuencia, tenga: «el incumplimiento de las obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales».

¹⁰¹ En estos casos, (con independencia de la obligación de vigilancia poscomercialización que corresponde a los fabricantes), estos podrán aducir la causa de exoneración basada en los riesgos del desarrollo siempre y cuando se den los requisitos para su aplicación y no derive el respectivo incidente o fallo de funcionamiento del producto del incumplimiento de las obligaciones en virtud del Derecho de la Unión destinadas precisamente a proteger frente a los daños producidos.

¹⁰² Véase art. 73.2 del RIA. Véase también art. 87.3 del Reglamento (UE) 2017/745.

riesgo y también, en su caso, la evaluación clínica, y deben atender, de este modo, al objetivo de transparencia.

7. CONCLUSIONES

Los sistemas de IA, en el ámbito sanitario, están demostrando ser una pieza clave para mejorar la salud y bienestar general de la población. Se utilizan, entre otros fines, para ayudar a mejorar la precisión de los diagnósticos, diseñar tratamientos personalizados, monitorizar la salud de los pacientes, identificar dianas terapéuticas y desarrollar nuevos fármacos, etc. Resulta crucial, en este sentido, que su implementación aborde todas aquellas cuestiones relacionadas con la seguridad y su buen funcionamiento.

En este trabajo, hemos planteado algunas de estas cuestiones cuando el producto es un sistema de IA utilizado con un fin médico específico (por ejemplo, para el diagnóstico basado en imagen médica). Hemos examinado que dicho sistema entra dentro del concepto de producto propuesto en la RLPEPDRPD. Por otra parte, dado que el análisis de dichos asuntos relativos a su seguridad y buen funcionamiento requiere conocer qué normativa resulta aplicable, hemos argumentado por qué dicho sistema es un producto sanitario y, asimismo, un sistema de IA de alto riesgo.

El sistema de IA utilizado para el diagnóstico es un producto sanitario que entra dentro del ámbito de aplicación del Reglamento (UE) 2017/745, y que procede clasificarlo como de alto riesgo en virtud del RIA, dado que dicho producto ha de someterse a un procedimiento de evaluación de la conformidad por un organismo independiente de acuerdo con dicho Reglamento (UE) 2017/745. De conformidad con la Regla 11 del anexo VIII, el sistema será clasificado, en su caso, en la Clase IIa o superior. Esto, asimismo, determinará el tipo de evaluación requerida (incluida la evaluación clínica) para obtener el marcado CE de conformidad, así como el seguimiento poscomercialización por el que se rige el producto. En dicho marcado CE el fabricante debe indicar que el producto es conforme con los requisitos aplicables del Reglamento (UE) 2017/745 y de otra legislación que resulte aplicable en su caso. Precisamente, al ser el producto sanitario un sistema de IA de alto riesgo deberá cumplir no sólo con todos los requisitos generales de seguridad y funcionamiento que, según el citado Reglamento le sean aplicables según su finalidad prevista (evaluación clínica debidamente documentada, los requisitos exigibles según su nivel de riesgo, etc.), sino también con los requisitos obligatorios establecidos para los sistemas de IA de alto riesgo (sección 2 del Capítulo III del RIA). En este caso, el fabricante de este producto se ajustará

al procedimiento de evaluación de la conformidad pertinente exigido por el Reglamento (UE) 2017/745. Los requisitos establecidos en la citada sección 2 del Capítulo III RIA se aplicarán al producto y formarán parte de dicha evaluación (art. 43.3 del RIA). Asimismo, se aplicarán los puntos 4.3, 4.4 y 4.5, 4.6, párrafo quinto, del anexo VII del RIA (art. 43.3). Según dispone este artículo, a efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo al Reglamento (UE) 2017/745 dispondrán de la facultad de controlar la conformidad del producto con los requisitos establecidos en la sección 2, (siempre que dichos organismos cumplan con los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11). Se exigen, entre otras cuestiones, que dichos organismos cuenten con personal (administrativo, técnico, jurídico y científico) que tenga experiencia y conocimientos relativos a los tipos de sistemas de IA, los datos y la computación de datos pertinentes y los requisitos establecidos en la sección 2. También, en cuanto al sistema de seguimiento poscomercialización, si ya se ha establecido un plan de vigilancia con arreglo al Reglamento (UE) 2017/745, el fabricante podrá optar por integrar los elementos descritos en los apartados 1, 2 y 3 del artículo 72 del RIA, utilizando el modelo señalado en el apartado 3, en los sistemas y planes que ya existen en virtud del Reglamento (UE) 2017/745, cuando se alcance un nivel de protección equivalente.

En el ámbito sanitario, donde puede haber repercusiones especialmente significativas para la vida y salud de las personas, los sistemas de diagnóstico y de apoyo a la toma de decisiones clínicas, (cuya sofisticación es cada vez mayor), deben ser fiables y precisos. Conocer que, a la luz de la normativa aplicable, el sistema de IA de alto riesgo cumple con los respectivos requisitos previstos en esta resulta esencial para prevenir debidamente los riesgos de seguridad que dicho sistema pueda generar. En este sentido, hemos visto que, precisamente, el cumplimiento de dichos requisitos será fundamental para apreciar si el sistema de IA es o no defectuoso. La noción de seguridad es un elemento clave para determinar la existencia de defecto. En la RLPEPDRPD el criterio para considerar un producto defectuoso sigue siendo, sustancialmente, el mismo: «cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional». Se amplían, no obstante, las circunstancias a tener en cuenta para valorar el carácter defectuoso de un producto, en concordancia, entre otros aspectos, con la naturaleza cambiante de los productos en la era digital.

En este trabajo hemos destacado algunas de dichas circunstancias en función de algunas características propias de nuestro producto sanitario que es también un sistema de IA de alto riesgo. Después de examinar qué podría determinar, en general, su carácter defectuoso (cuestión que implica cono-

cer la normativa aplicable), hemos visto que, precisamente, la demostración de que un producto no cumple con los respectivos requisitos obligatorios de seguridad establecidos en dicha normativa es una de las condiciones que la RLPEPDRPD prevé para, en su caso, presumir su carácter defectuoso.

En suma, el cumplimiento de dicha normativa aplicable al producto sanitario que es un sistema de IA de alto riesgo servirá como criterio, entre otros, para configurar las expectativas de seguridad que legítimamente cabe esperar por el público en general. También se verán afectadas las expectativas de los profesionales médicos que vayan a utilizarlo como soporte para la toma de sus decisiones clínicas. No obstante, el cumplimiento de dicha normativa no excluye el hecho de que dicho sistema de IA pueda ser defectuoso y causar daños. En este sentido, hemos visto que, tratándose de un complejo sistema de IA, la persona que reclame una indemnización por daños podría encontrarse en una situación de desventaja significativa frente a los operadores en cuanto al acceso a la información sobre cómo se ha diseñado dicho sistema, cómo funciona y en cuanto a la comprensión de dicha información. Dicha asimetría de la información puede, en estos casos de complejidad técnica o científica, menoscabar el reparto equitativo del riesgo. De este modo, hemos revisado también las medidas dirigidas a facilitar el acceso del demandante a las pruebas que vayan a utilizarse en los procesos judiciales y las presunciones que, bajo ciertas condiciones, servirán para aligerar la carga de la prueba.

Por último, en este trabajo hemos destacado una de las causas de exoneración de responsabilidad que podría alegar el fabricante de un innovador sistema de IA utilizado, por ejemplo, para el diagnóstico basado en imagen médica. Se trata de la denominada «exoneración basada en los riesgos del desarrollo». Supongamos que este sistema tuviera un fallo y causare daños al paciente, debido a que los conjuntos de datos de entrenamiento, validación y prueba, que eran adecuados y completos en vista de la finalidad prevista del sistema, se volvieran incompletos ante la aparición de nuevos tipos de patología que eran desconocidos en el momento de la modelización... ¿Estaría legitimado el fabricante del sistema de IA para exonerarse de responsabilidad en base a esta causa de exoneración? Como hemos señalado en este trabajo, para responder a esta cuestión, son varios los elementos de juicio que han de valorarse para su estimación. Con independencia de la obligación de vigilancia poscomercialización que corresponda a los fabricantes, estos podrán aducir esta causa de exoneración basada en los riesgos del desarrollo siempre y cuando se den los requisitos que hemos descrito para su aplicación y no derive el respectivo incidente o fallo del funcionamiento del sistema de IA del incumplimiento de las obligaciones que, en vir-

tud de la normativa aplicable, estaban destinadas precisamente a proteger frente a los daños ocasionados.

Resulta esencial, dados los múltiples beneficios que entraña la introducción de estos sistemas de IA en el ámbito sanitario, contar con dicho sistema de vigilancia poscomercialización, para tener en cuenta la experiencia con el uso de los mismos, perfeccionar, en su caso, su proceso de diseño y desarrollo, adoptar cualquier medida correctora, etc. Las conclusiones derivadas de cualquier acción preventiva y/o correctiva aplicada, servirán no sólo al objetivo de transparencia, sino también de mejora en la precisión de diagnósticos, la eficacia de tratamientos y la calidad de la asistencia sanitaria.

BIBLIOGRAFÍA

- Akay EMZ, Hilbert A, Carlisle BG, Madai VI, Mutke MA, Frey D. “Artificial Intelligence for Clinical Decision Support in Acute Ischemic Stroke: A Systematic Review”, *Stroke*, 2023, vol. 54, núm. 6, pp. 1505-1516.
- Ataz López, J. *Daños causados por las cosas: Una nueva visión a raíz de la robótica y de la inteligencia artificial*. Working paper 4/2020.
- Atienza Navarro, ML. “¿Una nueva responsabilidad por productos defectuosos?”, *InDret*, 2.2023, pp. 1-53.
- Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Madrid, 2022.
- Bercovitz Rodríguez-Cano, R. “La responsabilidad de los fabricantes en la Directiva de las Comunidades Europeas de 25 de junio de 1985”, *Estudios sobre consumo*, núm. 7, 1986.
- “Artículo 3”, en *Comentario del Texto Refundido de la Ley General para la defensa de los Consumidores y Usuarios y otras leyes complementarias*, Bercovitz, R., (Coord.), Aranzadi-Thomson Reuters, Cizur Menor, 2009, pp. 87-91.
- Bertolini, A. *Artificial Intelligence and civil liability*, 2020.
- BEUC (The European Consumer Organization). *Product Liability 2.0 How to make EU rules fit for consumers in the digital age*. Ref: BEUX-X-2020-024. 07/05/2020.
- Busto Lago, JM., Álvarez Lata, N., Peña López, F., *Reclamaciones de consumo. Derecho de consumo desde la perspectiva del consumidor*, Thomson Reuters Aranzadi, Cizur Menor, 2010.
- Cabral, TS. “Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive”, *Maastricht Journal of European and Comparative Law*, vol. 27, 5, 2020, pp. 615–635.
- Camacho Clavijo, S. *La telemedicina. Una aproximación a los distintos modelos de regulación en el marco europeo*, Madrid, Reus, 2024.

- Casadesus Ripoll, P. “Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos”, *Revista de la facultad de Derecho de México*, núm. 278, 2020, pp. 353-373.
- Dankwa-Mullan I, Rivo M, Sepulveda M, Park Y, Snowdon J, Rhee K. “Transforming Diabetes Care Through Artificial Intelligence: The Future Is Here”, *Popul Health Manag*, 2019, vol. 22, núm. 3, pp. 229-242.
- De Miguel Berian, I. “Medicina personalizada, algoritmos predictivos y utilización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos”, *Dilemata*, núm. 30, 2019, pp. 93-109.
- Debleena P, Gaurav S, Snehal S, et. al., “Artificial intelligence in drug discovery and development”, *Drug Discov Today*, vol. 26, núm. 1, 2021, pp. 80–93.
- European Law Institute, *Draft of a Revised Product Liability Directive. Draft Legislative Proposal of the European Law Institute*, 2022.
- Fundación Instituto Roche. Informe Anticipando: *Aplicaciones de la Inteligencia Artificial en Medicina Personalizada de Precisión*, 2023.
- Gil Membrado, C. *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*. VIII Premio Nacional de Derecho Sanitario, Madrid, Reus, 2023.
- Gómez ligüerre y García-Micó TG. “Liability for Artificial Intelligence and other emerging technologies”, *InDret*, 1, 2020, pp. 501-511.
- Grzybowski, A., Brona, P., Lim, G., et. al. “Artificial intelligence for diabetic retinopathy screening: a review”, *Eye*, vol. 34, 2020, pp. 451-460.
- Gutiérrez Santiago, P. *Daños causados por productos defectuosos*, Aranzadi, Cizur Menor, 2008.
- Hedderich DM, Weisstanner C, Van Cauter S, Federau C, Edjlali M, Radbruch A, et al. “Artificial intelligence tools in clinical neuroradiology: essential medico-legal aspects”, *Neuroradiology*, vol. 65, 2023, pp. 1091–1099.
- Herrera de la Heras, R. *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022.
- Howells, G., Twigg-flesner, Ch., Willett Ch. “Product Liability and Digital Products”, in Synodinou, TE., Jogleux, P., Markou, Ch., Prastitou, T. *EU Internet Law. Regulation and Enforcement*, Springer, 2017, pp. 183-195.
- Jorqui Azofra, M. *Responsabilidad por los daños causados por productos defectuosos y sistemas de inteligencia artificial*, en Moreno Martínez, JA. (Dir.), Dykinson, Madrid, 2023.
- Khurshid S. “Clinical perspectives on the adoption of the artificial intelligence-enabled electrocardiogram”, *Journal of Electrocardiology*, vol. 81, 2023, pp. 142-145.
- Koch AB, et. al. “Response of the European Law Institute to the Public Consultation on Civil Liability – Adapting Liability Rules to the Digital Age and Artificial Intelligence”, *Journal of European Tort Law*, vol. 13, 1, 2022, pp. 25-63.

- Lazcoz Moratinos, G. *Sistemas de inteligencia artificial en la asistencia sanitaria: cómo garantizar la supervisión humana desde la normativa de protección de datos*. <https://www.aepd.es/documento/premio-emilio-aced-2022-guillermo-lazcoz.pdf>
- Marín López, JJ. *Daños por productos: estado de la cuestión*, Tecnos, Madrid, 2001.
- Marín Salmerón, A. *El defecto de diseño en los productos digitales*, Aranzadi, Cizur Menor, 2023.
- Morris MX, Song EY, Rajesh A, Asaad M, Phillips BT. “Ethical, legal, and financial considerations of artificial intelligence in surgery”, *The American Surgeon*, 2023, vol 89, núm. 1, pp. 55–60.
- Navarro Michel, M. “Vehículos automatizados y responsabilidad por producto defectuoso”, *Revista de Derecho Civil*, núm. 5, 2020, pp. 175-223.
- Navas Navarro, S. *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022.
- Ngiam KY, Khor IW. “Big data and machine learning algorithms for health-care delivery”, *The Lancet Oncology*, 2019, vol. 20, núm. 5, pp. e262-e273.
- NÚÑEZ Zorrilla, MC. *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Reus, Madrid, 2019.
- Omiye JA, Gui H, Daneshjou R, Cai ZR, Muralidharan V. “Principles, applications, and future of artificial intelligence in dermatology”, *Frontiers in Medicine*, vol. 10, 2023.
- Parra Lucán, MA. “Artículo 133”, en Bercovitz Rodríguez-Cano, R (Coord.), *Comentario del texto refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias*, Cizur Menor, Aranzadi, 2015.
- “Artículo 137”, en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentario del texto refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias*, Cizur Menor, Aranzadi, 2015.
- Pinto, Imanol and Olazarán, Álvaro and Jurío, David and de la Osa, Borja and Sainz, Miguel and Oscoz, Aritz and Ballaz, Jerónimo and Gorricho, Javier and Galar, Mikel and Andonegui, José, “Improving Diabetic Retinopathy Screening Using Artificial Intelligence: Design, Evaluation and Before-and-After Study of an In-House Development”. Available at: SSRN: <http://dx.doi.org/10.2139/ssrn.4744622>
- Quaranta, M, Amantea, IA y Grosso, M. “Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double?”, *The Review of Socionetwork Strategies*, vol. 17, 2013, pp. 275-295.
- Ramos González, S. *Responsabilidad civil por medicamento. Defectos de fabricación, de diseño y en las advertencias o instrucciones*, Civitas, Madrid, 2004.
- Solé Feliu, J. *El concepto de defecto del producto en la responsabilidad civil del fabricante*, Tirant lo Blanch, Valencia, 1997.

Yousif M, Pantanowitz L. “Artificial intelligence-enabled gastric cancer interpretations: Are we there yet? *Surgical Pathology Clinics*, vol. 16, núm. 4, 2023, pp. 673-686.

NORMATIVA Y OTROS DOCUMENTOS

P9_TA(2024)0132. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

International Medical Device Regulators Forum, *Software as a Medical Device (SaMD): Key Definitions*, 2013, p. 6. Disponible en: <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>

Agencia Española de Medicamentos y Productos Sanitarios (AEMPS): <https://www.aemps.gob.es/informa/informacion-sobre-la-posibilidad-de-obtener-recomendaciones-de-dosis-de-insulina-incorrectas-al-utilizar-la-funcion-mentor-de-insulina-de-la-aplicacion-movil-onetouchreveal/>

Medical Devices coordination group (MDCG). MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

Reglamento (UE) 2017/745 del Parlamento europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo.

JURISPRUDENCIA

Tribunal de Justicia de la Unión Europea

STJUE 10 de junio de 2021 (C-65/20).

Tribunal Supremo

STS de 10 de junio de 2002 (RJ 2002/6198).

STS de 11 de junio de 2012 (RJ 2012/7330).

Audiencia Provincial

SAP Baleares de 19 de julio de 2000 (JUR 2000/296591).

SAP de Valencia de 12 de julio de 2001 (JUR 2001/279709).

SAP de Barcelona de 17 de diciembre de 2001 (JUR 2002/84388).

SAP de Cáceres de 18 de abril de 2002 (AC 2002/1330).

SAP de Zaragoza de 7 de marzo de 2003 (JUR 2003/110291).

SAP Barcelona de 13 de junio de 2005 (JUR 2005/ 181270).

SAP de Barcelona de 27 de septiembre de 2006 (AC 2006/1724).

SAP Palencia de 2 de noviembre de 2006 (AC 2006/105).

SAP de Barcelona de 16 de marzo de 2009 (AC 2009/1534).

SAP de Asturias de 24 de abril de 2009 (JUR 2009/283840).

IA y vehículos autónomos: cuestiones concernientes a la responsabilidad no contractual en la vertiente del derecho internacional privado¹

RAÚL LAFUENTE SÁNCHEZ

*Profesor titular de Derecho internacional privado,
Universidad de Alicante*

Sumario: 1. INTRODUCCIÓN. 2. VEHÍCULOS AUTÓNOMOS Y RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL. 2.1 Incidencia del Reglamento de Inteligencia Artificial. 2.1.1 Planteamiento. 2.1.2 ¿Es aplicable el Reglamento sobre IA a los vehículos automatizados? 2.1.3 Daños causados por los vehículos automatizados y posibles responsables. 2.2. Propuesta de revisión de la Directiva 85/374 sobre productos defectuosos. 2.2.1 Planteamiento. 2.2.2 Sistemas y productos de IA. 2.2.3 Responsabilidad por daños causados por productos defectuosos. A) Defectuosidad del producto. B) Personas responsables. C) Exención, reducción, exclusión o limitación de la responsabilidad. D) Carga de la prueba. 3. SOLUCIÓN DE CONTROVERSIAS Y APLICACIÓN DE LAS NORMAS DE DERECHO INTERNACIONAL PRIVADO. 3.1. Competencia judicial internacional. 3.1.1 Planteamiento. 3.1.2 El Reglamento Bruselas I bis. A) Foro general del domicilio del demandado. B) Competencias especiales en materia de obligaciones no contractuales. C) Foros de competencia en materia de seguros. a) Reclamaciones presentadas por el asegurador. b) Reclamaciones presentadas por la víctima. D) Competencia judicial internacional y acción directa. E) Autonomía de las partes para designar los tribunales competentes. 3.2 Ley aplicable. 3.2.1 Planteamiento. 3.2.2 El Reglamento Roma II. A) Autonomía de la voluntad de las partes y uso de sistemas de IA. B)

¹ Trabajo realizado al amparo del Proyecto “La Unión Europea ante los desafíos regulatorios de la Inteligencia Artificial: cuestiones de responsabilidad civil” - CIGE/2023/196 (Conselleria d'Educació, Cultura, Universitats i Ocupació de la Generalitat Valenciana).

Norma general: *lex loci damni* y accidentes de tráfico transfronterizos con vehículos automatizados. C) Ley aplicable a la responsabilidad por los daños causados por productos defectuosos. a) El artículo 5 del Reglamento Roma II. b) Responsabilidad por sistemas de IA defectuosos en la conducción automatizada. D) Reglas especiales. 3.2.3 Los Convenios de La Haya. A) El Convenio de La Haya de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera. B) El Convenio de La Haya de 1973 sobre Ley Aplicable a la Responsabilidad por Productos Defectuosos. 3.2.4 Conflictos que plantea la existencia y aplicación de diferentes instrumentos para determinar la ley aplicable. A) Ausencia de coordinación. B) Posibles soluciones. 3.2.5 Ventajas de aplicar el Reglamento Roma II frente a los Convenios de La Haya. 4. REFLEXIONES FINALES: IDONEIDAD DE LOS INSTRUMENTOS DE DIPR ACTUALMENTE EN VIGOR PARA REGULAR LAS RECLAMACIONES DERIVADAS DE LA CONDUCCIÓN AUTOMATIZADA. 4.1 Para determinar la jurisdicción de los tribunales de la UE. 4.2 En materia de ley aplicable. BIBLIOGRAFÍA

1. INTRODUCCIÓN

Hasta que se alcance la total incorporación de los vehículos automatizados en las carreteras, existirá una fase de transición durante la cual los vehículos con diferentes niveles de automatización compartirán las carreteras con los vehículos convencionales, conducidos por personas que no desean renunciar al placer de la conducción, o que por motivos económicos o por miedo no den el paso hacia los vehículos automatizados. Y la interacción entre ellos no será fácil, porque en estas condiciones de tráfico mixto pueden plantearse siniestros entre vehículos convencionales, entre vehículos automatizados y convencionales y entre vehículos autónomos, lo que puede generar que la conducción sea más insegura contrariamente al objetivo que se persigue con la automatización de los vehículos².

Como corolario, la coexistencia en las carreteras de distintos tipos de vehículos puede generar problemas a la hora de identificar los posibles responsables del accidente, ora los conductores o los proveedores de tec-

² DE BRUIN, R., "Autonomous Intelligent Cars on the European Intersection of Liability and Privacy: Regulatory Challenges and the Road Ahead", *European Journal of Risk Regulation*, vol. 7, n° 3, 2016, p. 495. Precisamente, el Parlamento Europeo, en su Resolución de 13 de marzo de 2018 sobre una estrategia europea sobre los sistemas de transporte inteligentes cooperativos, *doc. cit.*, apartado 14, pedía a la Comisión Europea que reflexionase sobre la manera de abordar la coexistencia de vehículos cooperativos, conectados y automatizados con vehículos y conductores no conectados, teniendo en cuenta que durante largo tiempo habrá un número importante de vehículos que seguirán sin estar conectados.

nología de estos vehículos, pues se trata de un aspecto novedoso por lo que respecta a las cuestiones de responsabilidad derivada de accidentes de tráfico.

Además, los sistemas de IA aplicados a la conducción serán capaces de desarrollar un funcionamiento autónomo y de adoptar decisiones sin la intervención humana o de una persona en concreto, es decir, pueden llevar a cabo un autoaprendizaje que impida su control por parte de los humanos y, en esos casos, pueden generar situaciones de riesgo y causar daños a terceros. En este contexto, hay que plantearse el alcance de la responsabilidad de estas máquinas (*electronic persons*) o agentes inteligentes, que carecen de personalidad jurídica y, por tanto, de capacidad para actuar y que tampoco disponen de un patrimonio propio, en aras a responder de las posibles responsabilidades, ni de un domicilio o de su correspondiente inscripción en un Registro público³.

Por lo tanto, en el futuro, las reclamaciones por la responsabilidad extracontractual derivada de estos accidentes ya no se sustentarán en la posible culpa o negligencia del conductor sino sobre los posibles defectos o el mal funcionamiento del producto, en particular, del sistema de IA instalado en el vehículo, a saber, el software o sistema operativo que realiza las tareas automatizadas del mismo.

En este sentido, hay que recordar que cuanto mayor sea el grado de automatización del vehículo mayor será el tiempo necesario para identificar el fallo y el responsable del accidente, con la consiguiente demora en la indemnización de las víctimas. Si a ello sumamos el tiempo adicional que puede ser necesario en caso de un litigio judicial, entenderemos que no son elementos que coadyuven a fortalecer la confianza del consumidor en el uso generalizado de este tipo de tecnología.

De ahí la importancia que tiene la aceptación de esta tecnología aplicada a la conducción por parte de los consumidores. Y los fabricantes, proveedores y otras partes implicadas en el proceso son conscientes de que sin la aceptación del consumidor no será posible el desarrollo y uso generalizado de los vehículos automatizados⁴.

³ EBERS, M., “La utilización de agentes electrónicos inteligentes en el tráfico jurídico ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?, InDret, 3, Julio 2016, pp. 16-17, disponible en <https://raco.cat/index.php/InDret/article/download/314400/404514/0>.

⁴ STANLEY, K. D., GRISÉ, M., y ANDERSON, J. M., “Autonomous vehicles and the future of Auto insurance”, Santa Monica, CA: RAND Corporation, 2020, pp. 60-61, disponible en https://www.rand.org/pubs/research_reports/RRA878-1.html

En consecuencia, para determinar la responsabilidad de los sistemas de IA instalados en los vehículos automatizados que puedan causar un daño de naturaleza no contractual a personas y bienes y, en particular, a sus responsables, hay que analizar de manera conjunta el Reglamento de IA⁵, y la Directiva sobre productos defectuosos, en su redacción dada por la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos⁶. Ello permitirá constatar cuando un sistema de IA puede catalogarse como un producto defectuoso y, a partir de ahí, identificar al responsable y las posibles vías de actuación ante los tribunales nacionales de la UE para solicitar la reparación de los daños.

Además, en el ámbito regulatorio y, en particular, respecto a la aplicación de las normas de Derecho internacional privado se plantean cuestiones de gran calado. Porque, al igual que sucede con los vehículos convencionales, los vehículos automatizados circularán por todo el territorio de la Unión Europea con independencia de su lugar de matriculación, la nacionalidad de sus ocupantes o la de las compañías aseguradoras. Y, en esos casos, surgirán conflictos de carácter transfronterizo ya que una gran parte de las reclamaciones que se planteen tendrán su origen en accidentes con elemento extranjero.

Por consiguiente, la identificación del responsable del daño será determinante con el fin de poder aplicar las normas de Derecho internacional privado y establecer los tribunales competentes y la ley aplicable a las reclamaciones que puedan plantear las víctimas. Pues no hay que olvidar que la generalización y el incremento exponencial del uso de los sistemas de IA en los vehículos puede generar, al menos en un primer momento, un aumento de conflictos de carácter transfronterizo que pueden acabar en reclamaciones por responsabilidad de carácter internacional tanto en el ámbito contractual cuanto en el extracontractual.

⁵ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) Texto pertinente a efectos del EEE (DOUE, L de 12.07.2024), disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

⁶ COM (2022) 495 final, de 28.09.2022, Vid., la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM (2022)0495 - C9-0322/2022 - 2022/0302(COD)), en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.pdf

2. VEHÍCULOS AUTÓNOMOS Y RESPONSABILIDAD CIVIL EXTRA-CONTRACTUAL

2.1 INCIDENCIA DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

2.1.1 Planteamiento

El pasado 12 de julio de 2024, se publicó en el DOUE el Reglamento de Inteligencia Artificial por el que se establecen normas armonizadoras en materia de Inteligencia Artificial y obligaciones a los operadores de sistemas IA.

Se trata de la primera normativa exhaustiva sobre IA, que tiene como objetivo fomentar una IA fiable en Europa y fuera de ella, garantizando que los sistemas de IA respeten los derechos fundamentales, la seguridad y los principios éticos. El Reglamento, que acoge un enfoque basado en el riesgo -lo que significa que cuanto mayor sea el riesgo de causar daños a la sociedad más estrictas serán las normas-, será de aplicación a partir del 2 de agosto de 2026⁷.

2.1.2 ¿Es aplicable el Reglamento sobre IA a los vehículos automatizados?

La incorporación de sistemas de IA en los vehículos de motor, los convertirá en máquinas o robots controladas por esta tecnología y diseñadas para desarrollar la función de la conducción de manera automatizada⁸.

De acuerdo con la clasificación universalmente aceptada efectuada en el año 2013 por la *Society of Automotive Engineers, SAE International*⁹ y adoptada en el año 2016 por la *National Highway Traffic Safety Administration (NHTSA)*¹⁰,

⁷ Artículo 113 del Reglamento de IA

⁸ La *National Highway Traffic Safety Administration (NHTSA)* define los vehículos automatizados del siguiente modo: “those in which at least some aspects of a safety-critical control function (for example, steering, throttle, or braking) occur without direct driver input.”. Vid., el documento “Preliminary Statement of Policy concerning Automated Vehicles” 1 (2013), en <https://www.nhtsa.gov/>

⁹ SAE International es una asociación profesional que tiene entre sus funciones el desarrollo de estándares para la industria de la ingeniería, con un enfoque especial en los sectores del transporte, como el automotriz, aeroespacial y de vehículos comerciales, y que tiene su sede en Estados Unidos, en Troy, Michigan y Warrendale, Pensilvania. Vid., <https://www.sae.org/> Vid., igualmente, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Standard J3016_202104 SAE International, en https://www.sae.org/standards/content/j3016_202104

¹⁰ United States Department of Transportation. Vid., <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>

existen distintos niveles de automatización de los vehículos, seis niveles que van de una escala de cero al cinco y que podrían cohabitar en el futuro dependiendo del grado de automatización que cada vehículo lleve integrado.

De ahí, la distinción entre automatización y autonomía: la primera, con una acepción más amplia, incluiría aquellos vehículos que asisten al conductor llevando a cabo todas las acciones previamente programadas, aunque sigue necesitando de la acción humana para los ajustes de su configuración, por ejemplo, en casos de avances tecnológicos; la segunda, la autonomía de los vehículos o conducción autónoma se predica de aquellos en los que todas las funciones están automatizadas y son llevadas a cabo por la tecnología, pudiendo tomar las decisiones adecuadas para completar las tareas asignadas sin la intervención humana. Técnicamente hablando, únicamente estos últimos podrían considerarse vehículos autónomos¹¹.

Pues bien, al objeto de establecer el marco regulatorio aplicable a los vehículos autónomos, la primera cuestión que se plantea es la posible aplicación del Reglamento de IA a los mismos. Para ello, hay que acudir a la definición que proporciona el Reglamento cuando se refiere a los sistemas de IA:

un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales¹²;

Así como al concepto de “riesgo” que define como “*la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio*”¹³.

A partir de ahí, el Reglamento identifica cuatro categorías de riesgo: sistemas de IA que pueden causar un riesgo inaceptable, en cuyo caso se trataría de prácticas de IA prohibidas¹⁴; sistemas de IA clasificados como sistemas de alto riesgo, en cuya aprobación quedaría sujeta al cumplimiento de requisitos legales específicos¹⁵; riesgo limitado, asociado a aquellas aplicaciones que no están explícitamente prohibidas o catalogadas como de alto riesgo y que

¹¹ HORVÁTHY, B., “*Autonomous vehicles - Challenges for EU private international law*”, EU Business Law and Digital, 2019, p. 4, disponible en http://real.mtak.hu/104981/1/Horvathy_autonomous%20vehicles.pdf

¹² Artículo 3 1) del Reglamento de IA.

¹³ *Ibidem*, artículo 3 2).

¹⁴ *Ibidem*, artículo 5.

¹⁵ *Ibidem*, artículos 6 y ss.

quedan en gran medida sin regular, si bien el Reglamento introduce obligaciones específicas de transparencia¹⁶; y, finalmente, aquellos que impliquen un riesgo mínimo o nulo, a los que el Reglamento no se refiere expresamente.

La cuestión, por tanto, será identificar los sistemas de IA que los vehículos autónomos lleven instalados y su posible encaje dentro de alguna de las categorías definidas por el Reglamento; en particular, si pueden considerarse como sistemas de alto riesgo sujetos al cumplimiento de los requisitos que la norma establece. En ese sentido, el Reglamento se refiere a los sistemas de alto riesgo del siguiente modo:

... un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación: a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos; y productos; y b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I¹⁷.

En mi opinión, los sistemas de IA incorporados en los vehículos de motor pueden catalogarse como sistemas de alto riesgo que van a ser utilizados “... como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión ...”¹⁸. Es decir, como componente de los vehículos de motor, que han de ser considerados como un producto que entra en el ámbito de los actos legislativos de armonización de la Unión Europea regulados en el Reglamento 2018/858¹⁹, y en el Reglamento 2019/2144 que modifica el anterior²⁰, tal y como dispone el Anexo I del Reglamento sobre IA.

¹⁶ *Ibidem*, artículos 1 d), 13 y 50.

¹⁷ *Ibidem*, artículo 6.1 a) y b).

¹⁸ *Ibidem*, artículo 6.1 letra a).

¹⁹ Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n° 715/2007 y (CE) n° 595/2009 y por el que se deroga la Directiva 2007/46/CE (DOUE L 151, de 14.06.2018)

²⁰ Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a

Además, el vehículo automatizado, como producto del que el sistema de IA es un componente de seguridad, ha de someterse “... a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión...”²¹.

Por consiguiente, los sistemas de IA instalados en los vehículos autónomos quedan sujetos a las disposiciones del Reglamento de IA que regula las obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes²².

2.1.3 Daños causados por los vehículos automatizados y posibles responsables

El incumplimiento de las obligaciones que impone el Reglamento de IA a los proveedores y responsables de sistemas de IA puede derivar en un incidente o defecto de funcionamiento del sistema de IA instalado en el vehículo -al que el Reglamento se define como “incidente grave”- y, en ese caso, causar daños a terceros con alguna de las siguientes consecuencias:

“incidente grave”: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias: a) el fallecimiento de una persona o un perjuicio grave para su salud; b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas, c) el incumplimiento de obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales, d) daños graves a la propiedad o al medio ambiente²³.

Con el fin de identificar a los responsables de los posibles daños causados por los sistemas de IA de alto riesgo, hay que considerar el alcance extraterritorial del Reglamento. Este, establece unos criterios de conexión muy amplios que afectan a todas las partes que, de alguna manera, puedan verse implicadas en la fabricación, distribución, introducción y despliegue de estos sistemas en el territorio de la Unión Europea. Se decanta, de este modo, por el principio

esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n° 78/2009, (CE) n° 79/2009 y (CE) n° 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 y (UE) 2015/166 de la Comisión (DOUE L 325, de 16.12.2019)

²¹ Artículo 6.1 letras a) y b) del Reglamento de IA.

²² *Ibidem*, artículos 16 y ss.

²³ *Ibidem*, artículo 3, apartado 49).

de la *lex loci damni*, es decir, la aplicación del Reglamento cuando el daño se haya producido en el territorio de la Unión y, al mismo tiempo, por su aplicación extraterritorial, lo que implica su aplicación a cualquier operador de sistemas de IA que tengan repercusión en la Unión Europea con independencia de su lugar de origen o establecimiento del proveedor²⁴.

Respecto a la reparación de los daños causados por los sistemas de IA el Reglamento dispone que:

... permanecen inalterados y siguen siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA, en particular en lo que respecta a la reparación de los posibles daños de conformidad con la Directiva 85/374/CEE del Consejo²⁵.

De ahí la importancia de analizar el mencionada Directiva y, en particular, las modificaciones introducidas por la propuesta de revisión actualmente en proceso.

2.2 PROPUESTA DE REVISIÓN DE LA DIRECTIVA 85/374 SOBRE PRODUCTOS DEFECTUOSOS

2.2.1 Planteamiento

Tras un largo proceso de consultas, en septiembre de 2022 la Comisión Europea presentó la Propuesta de Directiva por los daños causados por productos defectuosos²⁶. Esta, modificará y actualizará la Directiva 85/374 que ha venido aplicándose en el seno de la Unión Europea durante más de treinta

²⁴ *Ibidem*, artículo 2.1 que reza así: “Ámbito de aplicación: 1. El presente Reglamento se aplicará a: a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país; b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión; c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión; d) los importadores y distribuidores de sistemas de IA; e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca; f) los representantes autorizados de los proveedores que no estén establecidos en la Unión; g) las personas afectadas que estén ubicadas en la Unión”.

²⁵ Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (DO L 210, de 7.8.1985).

²⁶ COM (2022) 495 final, de 28.09.2022, *doc. cit.*

y cinco años, adaptando el marco legal a la creciente robotización y automatización de nuestra sociedad²⁷.

La Propuesta, pone de manifiesto la necesidad de que las empresas mejoren la seguridad de los productos y servicios vinculados a las tecnologías digitales, incluida la IA; de lo contrario, estos podrían causar daños y, en tales casos, ha de garantizarse el derecho de los perjudicados a una indemnización.

Se trata de una norma coherente con los instrumentos existentes en materia de responsabilidad, en particular con los regímenes nacionales de responsabilidad vigentes que permiten reclamar indemnizaciones a las personas responsables por los daños causados. No obstante, hay que señalar que, en esos casos, los demandantes tienen que demostrar la culpa de las personas responsables, lo que no se exige en la Directiva sobre responsabilidad por productos defectuosos, basada en un sistema de responsabilidad por riesgo creado (objetiva)²⁸.

La Propuesta “... establece normas comunes sobre la responsabilidad de los operadores económicos por los daños sufridos por personas físicas causados por productos defectuosos”²⁹, y pretende armonizar la legislación sobre responsabilidad civil en los Estados miembros, adaptando la norma anterior a las normas de seguridad de los productos y codificando la jurisprudencia del TJUE relativa a la Directiva sobre responsabilidad por productos defectuosos³⁰. De este modo, y con el fin de lograr un nivel de protección similar en todos los Estados miembros, no permite mantener o introducir en las legislaciones nacionales normas más o menos estrictas para alcanzar un nivel diferente de protección de los consumidores³¹.

Precisamente, en relación a uno de los aspectos que contempla la Propuesta de Directiva, la seguridad de los productos, hay que mencionar que ya existe un marco jurídico en la Unión Europea; a saber, el Reglamento relativo a la seguridad general de los productos, que deroga la Directiva 2001/95

²⁷ DE BRUYNE J. y WERBROUK, J., “Merging self-driving cars with the law”, *Computer Law & Security Review*, 34, 2018, pp. 1152, disponible en <https://daneshyari.com/article/preview/10225866.pdf>

²⁸ Por lo que respecta a las normas de la UE cabe citar, entre otras, la Directiva 2019/770, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales, y el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119, de 4.05.2016) (en adelante, el RGPD).

²⁹ Artículo 1 de la Propuesta de Directiva sobre responsabilidad por productos defectuosos.

³⁰ *Ibidem*, Exposición de motivos, Contexto de la Propuesta, apartado 1.1. Razones y objetivos de la propuesta.

³¹ *Ibidem*, artículo 3.

relativa a la seguridad general de los productos, anteriormente en vigor³². El Reglamento, incluye una nueva noción de “producto” que comprende aquellos que se encuentren interrelacionados con otros, como sucede en el caso de los productos que incorporan sistemas de IA; y, al mismo tiempo, distingue entre producto seguro y producto peligroso. Así dispone:

“producto”: todo objeto, esté interconectado o no con otros objetos, suministrado o puesto a disposición, a título oneroso o gratuito, incluso en el contexto de la prestación de un servicio, destinado a los consumidores o que, en condiciones razonablemente previsibles, pueda ser utilizado por los consumidores, aunque no esté destinado a ellos³³.

En fin, esta Propuesta se complementa con la Propuesta de Directiva sobre responsabilidad civil extracontractual en materia de IA, cuyo objetivo es facilitar el acceso de los demandantes a la información y aliviar la carga de la prueba en los casos de reclamación de indemnizaciones por daños causados por sistemas de IA. Pues la seguridad de los productos y la responsabilidad por los productos son dos aspectos complementarios para garantizar el buen funcionamiento del mercado interior. Por lo tanto, no existe solapamiento con las reclamaciones que puedan presentarse en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos³⁴.

2.2.2 Sistemas y productos de IA

Para adaptar el contenido de la actual Directiva sobre productos defectuosos a la realidad de los productos en la era digital -dado que pueden ser tangibles o intangibles-, entre los aspectos más relevantes introducidos por la Propuesta se encuentra la consideración de los sistemas de IA y los bienes habilitados para la IA como “productos”. Por tanto, entran dentro de su ámbito de aplicación y los daños causados por sistemas de IA defectuosos pueden

³² Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DOUE L 11, de 15.01.2002).

³³ *Vid.*, artículo 3, apartados 1) 2) y 3) del Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n° 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (DOUE L 135, de 23.05.2023). *Vid.*, al respecto, NÚÑEZ ZORRILLA, M. C., “Hacia un marco legal europeo uniforme en la prevención de los riesgos y de la responsabilidad civil en el ámbito de la conducción automatizada inteligente”, Cuadernos de Derecho Transnacional, vol. 15, n° 1, marzo 2023, p. 701.

³⁴ *Vid.*, la Exposición de motivos, apartados 1.2 y 1.3, de la Propuesta de Directiva sobre responsabilidad por productos defectuosos.

ser objeto de reclamación por parte de las personas perjudicadas sin que sea necesario demostrar la culpa del causante del daño. Incluye, por tanto, los archivos de fabricación digital y los programas informáticos (software) dentro de la definición de “producto”³⁵, y establece cuándo un servicio relacionado debe tratarse como componente de un producto³⁶. De todo ello cabe inferir que los sistemas de IA incorporados en los vehículos automatizados quedarán sujetos a las disposiciones de la Directiva que los Estados habrán de incorporar en sus respectivas legislaciones nacionales.

2.2.3 Responsabilidad por daños causados por productos defectuosos

A) Defectuosidad del producto

De acuerdo con la propuesta, un producto se considerará defectuoso cuando no proporcione la seguridad que un usuario tiene derecho a esperar, incluidos los requisitos de ciberseguridad pertinentes para la seguridad³⁷. Para determinar la defectuosidad, debe realizarse un análisis objetivo, tomando en consideración la finalidad prevista, las características objetivas y las propiedades del producto, así como las expectativas y requisitos de los usuarios a los que se destina el producto³⁸.

No obstante, existe una exclusión o excepción a esta regla y un producto no se considerará defectuoso por la única razón de que un producto mejor, incluidas las actualizaciones o mejoras de un producto, se comercialice ya o se ponga en servicio posteriormente³⁹.

³⁵ *Ibidem*, artículo 4 (1) and (2) donde define el archivo de fabricación digital como “una versión digital o plantilla digital de un bien mueble”. En este sentido, el Considerando 12 se refiere a la importancia de estos productos cuando señala que “Los programas informáticos, como los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos”; y el Considerando 14 a la posible defectuosidad de los mismos y de la protección del consumidor: “Los archivos de fabricación digital, que contienen la información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas, como taladros, tornos, molinos e impresoras 3D, deben considerarse productos, a fin de garantizar la protección de los consumidores en los casos en que esos archivos sean defectuosos”.

³⁶ *Ibidem*, artículo 4 (3), que define el componente como: “Cualquier artículo, tangible o intangible, o cualquier servicio conexo, que está integrado en un producto o interconectado con él por el fabricante de ese producto o que esté bajo su control”.

³⁷ *Ibidem*, artículo 6.1 f).

³⁸ *Ibidem*, Considerando 22.

³⁹ *Ibidem* artículo 6.2.

B) Personas responsables

En relación a las personas que pueden ser consideradas responsables de los daños, la Propuesta incluye, en primer lugar, a los fabricantes de hardware, a los proveedores de software y a los proveedores de servicios digitales que afectan al funcionamiento del producto (por ejemplo, en el ámbito de la conducción autónoma, el servicio de navegación que se instala en dichos vehículos). Del mismo modo, garantiza que los fabricantes puedan ser considerados responsables de los cambios que introduzcan en los productos que ya están en el mercado, incluso si esos cambios se deben a actualizaciones de software o al aprendizaje automático.

En este sentido, distingue según el tipo de operador implicado en cada caso. En primer lugar, determina que será responsable el fabricante del producto defectuoso. Para ello, considera que cualquier persona física o jurídica que modifique un producto ya comercializado o puesto en servicio en el transcurso de una actividad comercial será considerado como fabricante. No obstante, dicha modificación debe considerarse sustancial con arreglo a las normas pertinentes de la Unión o nacionales sobre seguridad de los productos y, además, que se haya realizado fuera del control del fabricante original. Además, cuando el defecto del producto haya sido causado por un componente defectuoso, el fabricante del componente también puede ser considerado responsable de los mismos daños⁴⁰.

En segundo lugar, regula la responsabilidad de los fabricantes establecidos fuera de la UE. En esos casos, hay que distinguir si el importador del producto defectuoso y el representante autorizado del fabricante están establecidos en el territorio de la Unión, pues entonces pueden ser considerados responsables de los daños causados por el producto defectuoso; pero, si ninguno de los dos estuviese establecido en la Unión Europea, el prestador de servicios de tramitación de pedidos a distancia puede ser considerado responsable de los daños causados por el producto defectuoso.⁴¹

En tercer lugar, en aquellos casos en los que no pueda establecerse la responsabilidad de los operadores antes mencionados -fabricante, importador,

⁴⁰ *Ibidem*, artículo 7, apartados 1 y 4.

⁴¹ *Ibidem*, artículo 7, apartados 2 y 3. En relación al concepto del “prestador de servicios de tramitación de pedidos a distancia”, *Vid.*, el artículo 4 14) que lo define del siguiente modo: “*toda persona física o jurídica que ofrezca, en el transcurso de su actividad comercial, al menos dos de los siguientes servicios: almacenar, embalar, dirigir y despachar un producto, sin tener la propiedad del producto en cuestión, con la excepción de los servicios postales, tal como se definen en el artículo 2, apartado 1, de la Directiva 97/67/CE del Parlamento Europeo y del Consejo, los servicios de paquetería, tal como se definen en el artículo 2, apartado 2, del Reglamento (UE) 2018/644 del Parlamento Europeo y del Consejo, y cualquier otro servicio postal o servicio de transporte de mercancías*”.

representante autorizado del fabricante o prestador del servicio de tramitación de pedidos a distancia-, la Propuesta prevé que los Estados miembros garantizarán que cada distribuidor del producto pueda ser considerado responsable siempre que se cumplan determinadas condiciones⁴².

La Propuesta también hace referencia a la contratación en línea. De este modo, establece que los proveedores de una plataforma en línea que permita a los consumidores celebrar contratos a distancia con comerciantes y que no sea un fabricante, importador o distribuidor también serán responsables, siempre que se cumplan las condiciones de la Ley de Servicios Digitales⁴³.

Por último, prevé la responsabilidad solidaria de aquellos operadores económicos (múltiples) que, de conformidad con las disposiciones de la Propuesta de Directiva, puedan ser considerados responsables del daño conjunta y solidariamente⁴⁴.

C) Exención, reducción exclusión o limitación de la responsabilidad

En la regulación de la responsabilidad de los operadores económicos vinculados con aquellos productos defectuosos que han causado daños, la Propuesta incluye la posibilidad de que estos operadores -fabricantes, importadores o distribuidores- queden excluidos de la responsabilidad por los daños causados por productos defectuosos siempre que acrediten la concurrencia de alguna de las siguientes circunstancias:

a) en el caso de un fabricante o importador, que no ha introducido el producto en el mercado ni lo ha puesto en servicio; b) en el caso de un distribuidor, que no ha comercializado el producto; c) que es probable que el defecto que causó el daño no existiera cuando el producto fue introducido en el mercado, puesto en servicio o, en el caso de un distribuidor, comercializado, o que este defecto se produjo después de ese momento; d) o que el defecto se debe a que el producto se ajusta a normas coercitivas dictadas por los poderes públicos; e) en el caso de un fabricante, que el estado objetivo de

⁴² *Ibidem*, artículo 7.5 que establece las siguientes condiciones: “a) que el demandante solicita al distribuidor que identifique al operador económico o a la persona que suministró el producto al distribuidor; y b) el distribuidor no identifique al operador económico o a la persona que suministró el producto al distribuidor en el plazo de un mes a partir de la recepción de la solicitud”.

⁴³ *Ibidem* artículo 7.6. *Vid.*, al respecto, Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DOUE L 277, de 27.10.2022)

⁴⁴ *Ibidem*, artículo 11.

los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o en el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso; f) en el caso de un fabricante de un componente defectuoso a que se hace referencia en el artículo 7, apartado 1, párrafo segundo, que el carácter defectuoso del producto sea imputable al diseño del producto a que se ha incorporado el componente o a las instrucciones dadas por el fabricante del producto al fabricante del componente; o g) en el caso de una persona que modifica un producto según lo dispuesto en el artículo 7, apartado 4, que el carácter defectuoso que haya causado el daño esté relacionado con una parte del producto no afectada por la modificación⁴⁵.

No obstante, en los casos a los que se refiere la letra c), la exención de responsabilidad del operador económico no se aplicará cuando la defectuosidad del producto se deba a alguna de las siguientes causas: un servicio conexo, programas informáticos, como el software, incluidas sus actualizaciones, o a la falta de actualización o mejoras de estos programas que sean necesarias para garantizar su seguridad. Y siempre que estas causas se encuentren bajo el control del fabricante⁴⁶.

En cuanto a la posible reducción de la responsabilidad por daños causados por productos defectuosos, la Propuesta prevé dos posibilidades; en primer lugar, la reducción de la responsabilidad o la exoneración de la misma cuando el daño sea causado tanto por el carácter defectuoso del producto como por la culpa del perjudicado o de un tercero del que éste sea responsable⁴⁷. En segundo lugar, obliga a los Estados miembros a no reducir la responsabilidad de los operadores económicos cuando el daño se deba tanto al carácter defectuoso del producto como a la acción u omisión de un tercero, sin distinguir si ese tercero tiene alguna relación con el operador⁴⁸.

Por último, la propuesta obliga a los Estados miembros a velar por que la responsabilidad de un agente económico en virtud de la presente Directiva no se vea limitada o excluida, en relación con la parte perjudicada, por una disposición contractual o por el Derecho nacional⁴⁹.

⁴⁵ *Ibidem*, artículo 10.1.

⁴⁶ *Ibidem*, artículo 10.2.

⁴⁷ *Ibidem*, artículo 12.2.

⁴⁸ *Ibidem*, artículo 12.1.

⁴⁹ *Ibidem*, artículo 13.

D) Carga de la prueba

Como principio general, la Propuesta de Directiva sobre responsabilidad por productos defectuosos establece la obligación del demandante de probar la defectuosidad del producto, el daño sufrido y el nexo causal entre la defectuosidad y el daño. Es decir, la carga de la prueba recae sobre la persona perjudicada⁵⁰.

Empero, la Propuesta trata de aliviar la carga de la prueba para el demandante en casos complejos, por ejemplo, en los relacionados con sistemas de IA y también cuando se trata de productos que no cumplen los requisitos de seguridad. Para ello, establece una presunción de defectuosidad del producto siempre que se cumpla alguna de las siguientes condiciones:

a) el demandado haya incumplido la obligación de exhibir las pruebas pertinentes de que disponga de conformidad con el artículo 8, apartado 1; b) el demandante demuestre que el producto no cumple los requisitos obligatorios de seguridad establecidos en el Derecho de la Unión o en la legislación nacional que tienen por objeto proteger contra el riesgo del daño que se ha producido; o c) el demandante demuestra que el daño fue causado por un mal funcionamiento evidente del producto durante el uso normal o en circunstancias normales⁵¹.

Respecto a la relación de causalidad, se presumirá su existencia entre la defectuosidad del producto y el daño causado cuando se haya constatado que el producto es defectuoso y el daño causado sea de un tipo compatible con el defecto en cuestión⁵².

Ahora bien ¿qué ocurrirá si el demandante no puede probar la defectuosidad del producto o la relación entre el defecto y el daño causado? En tales casos, si los tribunales nacionales consideran que el demandante se enfrenta a dificultades excesivas en relación con la carga de la prueba -debido a dificultades técnicas o científicas-, la Propuesta considera que existirá una presunción de defectuosidad y de relación causal siempre y cuando el demandante haya demostrado que: “a) *el producto contribuyó a los daños*; y b) *es probable que el producto sea defectuoso o que su carácter defectuoso sea una causa probable de los daños, o ambos*”⁵³.

⁵⁰ *Ibidem*, artículo 9.1.

⁵¹ *Ibidem*, artículo 9.2.

⁵² *Ibidem*, artículo 9.3.

⁵³ *Ibidem* artículo 9.4.

En cualquier caso, el demandado tendrá derecho a impugnar la existencia de dificultades excesivas para probar la defectuosidad del producto o el nexo causal entre defecto y daño, de tal forma que el perjudicado se vea obligado a probar la misma; así como el derecho a refutar cualquiera de las presunciones establecidas anteriormente⁵⁴.

3. SOLUCIÓN DE CONTROVERSIAS Y APLICACIÓN DE LAS NORMAS DE DERECHO INTERNACIONAL PRIVADO

3.1 COMPETENCIA JUDICIAL INTERNACIONAL

3.1.1 Planteamiento

En el nuevo escenario que se vislumbra con la aplicación de la IA a la conducción automatizada, se van a seguir planteando situaciones en las que el Estado del domicilio del infractor, el Estado donde tenga lugar el accidente y el Estado de registro o matriculación del vehículo sean diferentes, por lo que hay que analizar los instrumentos de Derecho internacional privado actualmente en vigor aplicables al régimen de responsabilidad civil extracontractual en materia de accidentes de tráfico transfronterizos.

Empero, la incorporación de los sistemas de IA como elemento integrante de los vehículos autónomos que puedan verse implicados en un accidente de tráfico transfronterizo y, por ende, en la responsabilidad derivada de los daños causados, genera algunas dudas respecto a la aplicación de las normas e instrumentos en vigor para determinar la competencia de los tribunales de la Unión Europea cuando, por ejemplo, el producto defectuoso origen del daño sea un sistema de IA.

Porque, en estos casos, desde la perspectiva del Derecho internacional privado la responsabilidad por productos defectuosos adquiere mayor relevancia y, al objeto de determinar la jurisdicción internacional de los tribunales, no se considera como una categoría específica, sino que se le aplican los foros de competencia previstos para las obligaciones no contractuales.

Por este motivo, como algún autor ha sugerido, tal vez el criterio del *loci damni* no sea el más apropiado para determinar el foro competente, ni desde

⁵⁴ *Ibidem*, artículo 9, apartados 4 y 5.

la perspectiva legal ni desde la económica, porque plantea dudas a la hora de aplicarlo a los casos de responsabilidad por productos en el ámbito de los sistemas de IA⁵⁵.

En cualquier caso, habrá que seguir acudiendo al Reglamento 1215/2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil⁵⁶, con independencia de la naturaleza del órgano jurisdiccional y teniendo en cuenta la exclusión de ciertas materias de su ámbito de aplicación que el propio Reglamento establece⁵⁷. Por otra parte, conviene recordar que el Reglamento no contienen normas específicas en materia de accidentes de tráfico transfronterizos, por lo que seguirá existiendo este mismo vacío respecto a los conflictos que se planteen en el marco de la conducción de vehículos autónomos.

3.1.2 El Reglamento Bruselas I bis

A) Foro general del domicilio del demandado

Por lo que respecta a la determinación de la jurisdicción de los tribunales, el Reglamento se aplicará siempre que la parte demandada se encuentre domiciliada en el territorio de la Unión Europea, con independencia de su nacionalidad⁵⁸. Por lo tanto, se trata del criterio que delimita la aplicación territorial del mencionado Reglamento, siendo la norma general para determinar la jurisdicción de los tribunales de la UE que refleja el principio *actor sequitur forum rei*. Además, la elección del criterio del domicilio frente al de la

⁵⁵ CAPPIELLO, B., *AI-systems and non-contractual liability. A european private international law analysis*, Giappichelli Editori, Torino, 2022, pp. 100 y 105.

⁵⁶ Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DOUE L 351, de 20.12.2012) (*en adelante, el Reglamento Bruselas I bis*). No será objeto de tratamiento en esta monografía el Convenio de Lugano cuyas normas se ajustan a las del Reglamento Bruselas I bis a fin de lograr el mismo nivel de circulación de resoluciones judiciales entre los Estados miembros de la UE y los Estados de la AELC interesados, y que se aplica a la UE, Dinamarca y los Estados de la AELC. *Vid.*, la Decisión del Consejo de la Unión Europea, de 15 de octubre de 2007, relativa a la firma, en nombre de la Comunidad, del Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DOUE L 339, de 21.12.2007).

⁵⁷ *Ibidem*, artículo 1.2, que se refiere, en particular, a las materias fiscal, aduanera administrativa y a la responsabilidad del Estado por acciones u omisiones en el ejercicio de su autoridad (*acta iure imperii*).

⁵⁸ *Ibidem*, artículo 4.

residencia habitual hace que la aplicación de esta norma de competencia revista un alto grado de previsibilidad⁵⁹.

Así, en el ámbito de las reclamaciones extracontractuales derivadas de la conducción automatizada, seguirá operando el foro del domicilio del demandado cuando este se encuentre en el territorio de la Unión Europea; ya sea en casos de demandas iniciadas contra el conductor, el propietario, el fabricante o la empresa que ha desarrollado el software del vehículo automatizado causante del siniestro.

Con el fin de determinar el domicilio de una persona física, el tribunal que conozca del asunto aplicará su ley interna, pero, si la demandada no estuviese domiciliada en el Estado miembro cuyo tribunal conoce del asunto, para determinar si está domiciliada en otro Estado miembro, aplicará la ley de dicho Estado miembro⁶⁰.

Por su parte, cuando la demandada sea una persona jurídica, el Reglamento permite tres opciones con el fin de determinar donde se encuentra su domicilio, a saber: el lugar donde se encuentre su sede estatutaria, su administración central o su centro de actividad principal⁶¹. En cualquier caso, ese domicilio debe definirse de manera autónoma para incrementar la transparencia de las normas comunes y evitar los conflictos de jurisdicción⁶².

Pues bien, esa triple opción que plantea el Reglamento otorga al reclamante la opción de elegir entre los tribunales de la UE que estén vinculados con los criterios antes señalados y, además, permite localizar el domicilio de una persona jurídica en el territorio de la UE, por ejemplo, por la localización de su administración central aun cuando hubiese trasladado su sede estatutaria fuera de la Unión.

Por el contrario, cuando la parte demandada, ya sea persona física o jurídica, no se encuentre domiciliada en el territorio de la Unión, de acuerdo a los criterios antes señalados, la jurisdicción de los tribunales se determinará con arreglo a la legislación interna de cada Estado miembro⁶³.

B) Competencias especiales en materia de obligaciones no contractuales

Con el fin de contribuir y facilitar una buena administración de justicia, el Reglamento Bruselas I bis dispone que el foro del domicilio del demandado debe completarse con otros foros alternativos a causa de la estrecha co-

⁵⁹ *Ibidem*, Considerando 15.

⁶⁰ *Ibidem*, artículo 62.

⁶¹ *Ibidem*, artículo 63.

⁶² *Ibidem*, Considerando 15.

⁶³ *Ibidem*, artículo 6.

nexión existente entre el órgano jurisdiccional y el litigio⁶⁴. De este modo, Reglamento prevé que, en determinadas circunstancias, también podrán declararse competentes los tribunales de otro Estado miembro distinto al del domicilio del demandado.

Así, en el ámbito de las reclamaciones de carácter extracontractual, el Reglamento establece un foro de competencia especial que distingue claramente del foro de competencia en materia de obligaciones contractuales⁶⁵. Para ello, se refiere a la materia delictual o cuasidelictual, lo que incluye todos los casos de responsabilidad no contractual, ya deriven de culpa, de responsabilidad objetiva o de responsabilidad por productos⁶⁶. Ahora bien, tal y como el TJUE ya ha declarado “*la responsabilidad delictual o cuasidelictual sólo surge cuando pueda establecerse un nexo causal entre el daño y el hecho que lo origina*”⁶⁷.

Por consiguiente, con arreglo a la norma de competencia prevista para las obligaciones no contractuales, el Reglamento otorga competencia internacional y territorial de manera inmediata a los tribunales del Estado miembro en el que se localice el lugar donde se haya producido o pueda producirse el hecho dañoso.

Este concepto del *locus commissi delicti* ha sido interpretado por el TJUE de una manera amplia, al considerar que incluye tanto el lugar donde ocurrió el acto desencadenante cuanto el lugar donde se materializó el daño y se sufrieron las consecuencias. Doble fórum -*locus damni* y *locus actus*-, o teoría de la ubicuidad, que permite a la víctima elegir si demanda ante los tribunales del Estado miembro donde se hubiese producido o donde pudiese producirse el hecho dañoso siempre que se trate de un daño directo, y que favorece que el tribunal que se declare competente sea el que se encuentra en mejor disposición para conocer de la demanda⁶⁸. Pues, tal y como ha señalado el TJUE “... *tanto el lugar del hecho causante, como el lugar en que se materializa el daño, pueden constituir, según los casos, una conexión relevante desde el punto de vista de la competencia judicial*”⁶⁹.

⁶⁴ *Ibidem*, Considerando 16.

⁶⁵ *Ibidem*, artículo 7.2 en contraposición con al artículo 7.1.

⁶⁶ *Vid.*, DAVÌ, A., *La responsabilità extracontrattuale*, UTET, Torino, 1997, p. 107; FRANZINA, P., *La giurisdizione in materia contrattuale. L'art. 5 n° 1 del Regolamento n. 44/2001 CE nella prospettiva dell'armonia delle decisioni*, CEDAM, Padova, 2006, p. 177; y MARI, L., *Il diritto processuale civile della Convenzione di Bruxelles. Il sistema della competenza*, CEDAM, Padova, 1999, p. 376.

⁶⁷ Sentencia del TJUE de 28 de julio de 2013, asunto C-147/12, *ÖFAB*, ECLI:EU:C:2013:490, párrafo 34, en el que citaba sus decisiones de 30 de noviembre de 1976, asunto 21/76, *Handelskwekerij Bier/Mines de Potasse d'Alsace* Rec. p.1735, párrafo 16; y de 16 de julio de 2009, asunto C-189/09, *Zuid-Chemie*, Rec. p. I-6917, párrafo 28.

⁶⁸ *Vid.*, al respecto, las Sentencias del TJUE de 30 de noviembre de 1976, asunto C-21/76, *Handelskwekerij Bier/Mines de Potasse d'Alsace*, ECLI:EU:C:1976:166; y de 11 de enero de 1990, asunto C-220/88, *Dumez France and Others v Hessische Landesbank and Others*, ECLI:EU:C:1990:8.

⁶⁹ Sentencia del TJUE, asunto C-21/76 - *Handelskwekerij Bier/Mines de Potasse d'Alsace*, cit. párrafo 15.

De este modo, en el ámbito de las reclamaciones por siniestros en los que se vean implicados vehículos autónomos resulta de especial interés esta interpretación porque permite a las víctimas demandar ante los tribunales del Estado miembro del lugar donde se haya producido el hecho causante o donde se haya materializado el daño. A su vez, esta interpretación permite a la parte demandada prever los foros alternativos ante los que podría ser demandada.

En fin, cuando esa reclamación de responsabilidad derive de un acto que dé lugar a un proceso penal, también será competente el tribunal que conozca sobre este proceso⁷⁰.

C) Foros de competencia en materia de seguros

Junto a las normas de competencia ya analizadas -la general del domicilio del demandado y las especiales en materia de obligaciones no contractuales- hay que señalar las normas de competencia en materia de seguros previstas en el Reglamento Bruselas I bis. Porque, al igual que sucede en la actualidad, la obligación de aseguramiento de todo vehículo matriculado en la Unión Europea habrá de hacerse extensible a los vehículos automatizados. Y, en este sentido, el Reglamento diseña un sistema de foros de competencia que prevalecerán sobre los anteriormente indicados.

La finalidad de este sistema es proteger a la parte débil, considerando la desigualdad existente en estos tipos de contratos internacionales donde una de las partes cocontratantes (el asegurador) se encuentran en una posición prevalente frente a la otra parte -el tomador del seguro, el asegurado, el beneficiario y/o el perjudicado-, considerada la parte débil. Y así, incorpora normas de competencia más favorables a los intereses de estos últimos⁷¹.

La competencia judicial en materia de seguros se determinará, pues, en función de estas disposiciones, sin perjuicio de lo dispuesto en los artículos 6 y 7.5 del Reglamento⁷². Y variará en función de la parte que ostente la legitimación activa para demandar.

⁷⁰ Artículo 7.3 del Reglamento Bruselas I bis.

⁷¹ *Ibidem*, Considerando 18. Estas normas se establecen en la Sección 3, Competencia en materia de seguros, artículos 10 al 16.

⁷² *Ibidem*, artículo 6, que se refieren a la determinación de la competencia de conformidad con la legislación interna de los Estados miembros cuando el demandado no se encuentre domiciliado en territorio del Reglamento Bruselas I bis; y artículo 7.5, que regula la competencia de los tribunales del lugar en el que se encuentre la sucursal o agencia cuando se trate de un litigio relativo a la explotación de tales establecimientos.

a) Reclamaciones presentadas por el asegurador

Así, cuando la reclamación la presente la compañía aseguradora contra el tomador, el asegurado o el beneficiario del seguro, los tribunales competentes serán los del domicilio del demandado en la Unión Europea⁷³ (criterio del domicilio del demandado coincidente con el principio general establecido en el artículo 4 del Reglamento Bruselas I bis).

b) Reclamaciones presentadas por la víctima

Sin embargo, cuando la acción sea ejercitada por el tomador del seguro, el asegurado, el beneficiario o el perjudicado, contra la compañía aseguradora o coaseguradora domiciliada en un Estado miembro, el abanico de posibilidades se amplía y el Reglamento contempla diversos foros.

En primer lugar, los tribunales del domicilio del demandado -compañía aseguradora-⁷⁴; en segundo lugar, cuando se trate de seguros de responsabilidad, el asegurador también podrá ser demandado ante los tribunales del lugar en el que se haya producido el hecho dañoso⁷⁵; y, en tercer lugar, el tomador del seguro, el asegurado, el beneficiario y/o la persona perjudicada -tal y como ha tenido ocasión de establecer el TJUE en su jurisprudencia-⁷⁶, también podrán presentar la demanda ante los tribunales del Estado miembro en los que tengan su domicilio (*forum actoris*)⁷⁷, pues el Reglamento Bruselas I bis contempla la posibilidad de que la persona perjudicada pueda entablar la acción directa contra la compañía aseguradora, siempre que dicha acción sea posible⁷⁸.

D) Competencia judicial internacional y acción directa

En este escenario, reviste gran importancia el ejercicio de la acción directa contra el asegurador del responsable, ya que permite al perjudicado re-

⁷³ *Ibidem* artículo 14, que reza así: “1. Salvo lo dispuesto en el artículo 13, apartado 3, la acción del asegurador solo podrá ser ejercitada ante los órganos jurisdiccionales del Estado miembro en cuyo territorio esté domiciliado el demandado, ya sea tomador del seguro, asegurado o beneficiario”.

⁷⁴ *Ibidem*, artículo 11.1 a).

⁷⁵ *Ibidem*, artículo 12. Este foro se corresponde con el previsto en el artículo 7.2 del Reglamento

⁷⁶ Sentencia del TJUE, de 13 de diciembre de 2007, asunto C-463/06, *FBTO Schadeverzekering*, ECLI:EU:C:2007:792.

⁷⁷ Artículos 11, 12 y 13 del Reglamento Bruselas I bis, en particular, el artículo 11 que dispone: “El asegurador domiciliado en un Estado miembro podrá ser demandado: a) ante los órganos jurisdiccionales del Estado miembro donde tenga su domicilio; b) en otro Estado miembro, cuando se trate de acciones entabladas por el tomador del seguro, el asegurado o un beneficiario, ante el órgano jurisdiccional del lugar donde tenga su domicilio el demandante, ...”.

⁷⁸ *Ibidem*, artículo 13.2 en relación con los artículos 10, 11 y 12. *Vid.*, en este sentido, la doctrina del TJUE en materia de personas perjudicadas, en su Sentencia de 13 de diciembre de 2007, asunto C-463/06, *FBTO Schadeverzekering*, *cit.*

clamarle directamente por los daños ocasionados. Su ejercicio será posible cuando así lo disponga la ley aplicable a la obligación extracontractual o la ley aplicable al contrato de seguro, tal y como dispone el Reglamento Bruselas I bis⁷⁹.

Y no hay que olvidar que esta misma acción viene contemplada en los instrumentos de Derecho internacional privado para determinar la ley aplicable, tanto en el texto del Reglamento Roma II relativo a la ley aplicable a las obligaciones extracontractuales⁸⁰, cuanto en el Convenio de La Haya de 1971 sobre Ley aplicable en materia de accidentes de circulación por carretera⁸¹, a los que más adelante me referiré.

A mayor abundamiento, la Directiva 2009/103, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles⁸², que vino a codificar las anteriores Directivas sobre el seguro de automóviles⁸³, establece la obligación de los Estados miembros de garantizar que las partes

⁷⁹ Vid., el artículo 13.2 en relación al 11.1. b) del Reglamento Bruselas I bis, que dispone: “Los artículos 10, 11 y 12 serán aplicables en los casos de acción directa entablada por la persona perjudicada contra el asegurador cuando la acción directa sea posible”.

⁸⁰ El artículo 18 del Reglamento (CE) n° 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales (Roma II) (DOUE L 199, de 31.7.2007) (en adelante, el Reglamento Roma II) establece: “La persona perjudicada podrá actuar directamente contra el asegurador de la persona responsable para reclamarle resarcimiento si así lo dispone la ley aplicable a la obligación extracontractual o la ley aplicable al contrato de seguro”.

⁸¹ El artículo 9 del Convenio de La Haya de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera, hecho en La Haya el 4 de mayo de 1971 (Instrumento de ratificación publicado en el BOE núm. 264, de 4 de noviembre de 1978) (en adelante, el Convenio de La Haya de 1971) reza así: “Las personas perjudicadas tendrán derecho a actuar directamente contra el asegurador del responsable, si ese derecho les es reconocido por la ley aplicable conforme a lo dispuesto en los artículos 3, 4 o 5”.

⁸² Directiva 2009/103/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad (Texto pertinente a efectos del EEE) (DOUE L 263, de 7.10.2009).

⁸³ Las cinco directivas sobre el seguro de automóviles adoptadas desde 1972 son las siguientes: la Directiva 72/166/CEE del Consejo, de 24 de abril de 1972, relativa a la aproximación de las legislaciones de los Estados miembros, sobre el seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como del control de la obligación de asegurar esta responsabilidad (DO L 103 de 2.5.1972); la Segunda Directiva 84/5/CEE del Consejo, de 30 de diciembre de 1983, relativa a la aproximación de las legislaciones de los Estados miembros sobre el seguro de responsabilidad civil que resulta de la circulación de los vehículos automóviles (DO L 8 de 11.1.1984); la Tercera Directiva 90/232/CEE del Consejo, de 14 de mayo de 1990, relativa a la aproximación de las legislaciones de los Estados miembros sobre el seguro de responsabilidad civil derivada de la circulación de vehículos automóviles (DO L 129 de 19.5.1990), la Directiva 2000/26/CE del Parlamento Europeo y del Consejo, de 16 de mayo de 2000, relativa a la aproximación de las legislaciones de los Estados miembros sobre el seguro de responsabilidad civil derivada de la circulación de vehículos automóviles (Cuarta Directiva sobre el seguro de vehículos automóviles) (DO L 181 de 20.7.2000); y la quinta Directiva 2005/14/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, por la que se modifican las Directivas 72/166/CEE, 84/5/CEE, 88/357/CEE y 90/232/CEE del Consejo

perjudicadas en un accidente causado por un vehículo cubierto por el seguro de responsabilidad civil relativa a la circulación de vehículos tengan derecho a interponer una acción directa contra la empresa de seguros que cubre a la persona responsable en lo que respecta a la responsabilidad civil⁸⁴.

De tal forma que, una vez incorporada la Directiva en los ordenamientos jurídicos nacionales, la acción directa se podrá ejercitar siempre que la ley aplicable a la responsabilidad extracontractual derivada de un accidente de tráfico transfronterizo sea la ley de un Estado miembro. En el caso español, la mencionada Directiva se encuentra incorporada a través de la Ley 50/1980, de Contrato de Seguro⁸⁵ y del Real Decreto Legislativo 8/2004, Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor⁸⁶, normas en las que, expresamente, se hace mención al ejercicio de la acción directa por parte del perjudicado o sus herederos frente al asegurador.

E) Autonomía de las partes para designar los tribunales competentes

Por otro lado, el Reglamento Bruselas I bis establece que ha de respetarse la autonomía de la voluntad de las partes y permite que estas puedan elegir el tribunal competente (*prorogatio fori*), siempre dentro de los límites y condiciones que establece el propio Reglamento y respetando los criterios establecidos en las normas específicas de jurisdicción antes señaladas⁸⁷. Es cierto, sin embargo, que se refiere a la autonomía de las partes en el marco contractual⁸⁸; por tanto, en los supuestos de responsabilidad extracontractual derivada de los daños causados por sistemas de IA y, en particular, de la conducción

y la Directiva 2000/26/CE del Parlamento Europeo y del Consejo relativas al seguro de responsabilidad civil derivada de la circulación de vehículos automóviles (DO L 149, de 11.6.2005).

⁸⁴ *Vid.*, el artículo 16, en relación al artículo 3, de la Directiva relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles.

⁸⁵ El artículo 76 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (BOE n°. 250, de 17.10.1980), dispone: “*El perjudicado o sus herederos tendrán acción directa contra el asegurador para exigirle el cumplimiento de la obligación de indemnizar, sin perjuicio del derecho del asegurador a repetir contra el asegurado, en el caso de que sea debido a conducta dolosa de éste, el daño o perjuicio causado a tercero. La acción directa es inmune a las excepciones que puedan corresponder al asegurador contra el asegurado. El asegurador puede, no obstante, oponer la culpa exclusiva del perjudicado y las excepciones personales que tenga contra éste. A los efectos del ejercicio de la acción directa, el asegurado estará obligado a manifestar al tercero perjudicado o a sus herederos la existencia del contrato de seguro y su contenido.*”

⁸⁶ El artículo 7 del Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor (LRCSCVM) (BOE n° 267, de 05.11.2004) dispone: “*El perjudicado o sus herederos tendrán acción directa para exigir al asegurador la satisfacción de los referidos daños, que prescribirá por el transcurso de un año.*”

⁸⁷ *Vid.*, los artículos 25 y 26 del Reglamento Bruselas I bis.

⁸⁸ *Ibidem*, Considerando 19.

de vehículos automatizados, la designación del tribunal competente por las partes ha de matizarse.

En primer lugar, la sumisión expresa o pacto atributivo de competencia tendrá que producirse *ex post*, es decir, con posterioridad al nacimiento del litigio, pues las partes que se ven implicadas en una reclamación de naturaleza no contractual no suelen tener una relación previa que les permita efectuar el pacto con anterioridad⁸⁹.

Lo mismo sucede respecto a la sumisión tácita, que tendrá lugar con posterioridad al hecho dañoso cuando una de las partes, la víctima, acuda ante un tribunal de la Unión Europea y la demandada comparezca ante el mismo para responder al fondo del asunto⁹⁰.

En segundo lugar, la elección del tribunal competente por las partes solamente será válido en la medida en que ambas partes se encuentren en igualdad de condiciones -por ejemplo, en una reclamación entre propietarios de vehículos automatizados intervinientes en un accidente- o, de no ser así, cuando el pacto proteja a la parte débil en la reclamación extracontractual -por ejemplo, a la víctima frente al fabricante del vehículo automatizado, el proveedor de servicios de software del vehículo automatizado o la compañía aseguradora del mencionado vehículo⁹¹.

3.2 LEY APLICABLE

3.2.1 Planteamiento

Para determinar la ley aplicable en casos de responsabilidad no contractual derivada de accidentes de tráfico transfronterizos, el lugar de producción del daño (*lex loci damni*) es el punto de conexión que se ha venido utilizando con carácter preferente, tal y como establece el Reglamento 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales. Así sucede también con otras obligaciones de naturaleza extracontractual -daños por actos de competencia desleal, daños medioambientales o infracciones de derechos de propiedad intelectual, ... entre otras⁹².

Empero, en esta materia no existe unificación de normas de conflicto en la Unión Europea, por lo que el Reglamento Roma II coexiste con la apli-

⁸⁹ *Ibidem*, artículo 25.

⁹⁰ *Ibidem*, artículo 26.

⁹¹ *Ibidem*, artículos 10 y ss, Competencia en materia de seguros.

⁹² *Vid.*, los artículos 6 al 12 del Reglamento Roma II.

cación de dos Convenios internacionales, el Convenio de La Haya de 1971, sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera⁹³ y el Convenio de La Haya de 1973, sobre Ley Aplicable a la Responsabilidad por Productos⁹⁴. Ello no empece para que pueda analizarse y, en su caso, sugerir la posible actualización de este marco jurídico con el fin de dar respuesta a los problemas que surjan al socaire del régimen de responsabilidad civil extracontractual en el futuro a raíz de la participación de vehículos automatizados en los accidentes de tráfico transfronterizos.

3.2.2 El Reglamento Roma II

El Reglamento Roma II establece normas uniformes con el fin de determinar la ley aplicable a las obligaciones no contractuales, contribuyendo así a garantizar el buen funcionamiento del mercado interior y favoreciendo que las normas de conflicto de leyes vigentes en los Estados miembros designen la misma ley nacional con independencia del tribunal de la Unión Europea ante el que se haya planteado el litigio⁹⁵.

Respecto a su ámbito de aplicación material, hay que recordar, no obstante, que no será de aplicación a las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad, en particular, la difamación⁹⁶, en definitiva, infracciones relacionadas con la privacidad que en el ámbito de los sistemas de IA aplicados a la conducción automatizada pueden plantearse con el tratamiento de datos personales a los que estos sistemas tengan acceso. Por lo tanto, en ausencia de cobertura por parte del Reglamento Roma II habrá que acudir a las normas de conflicto nacionales de cada Estado.

Por otra parte, el Reglamento considera como “daños” todas las consecuencias derivadas de un hecho dañoso y, además, se aplicará a las obligaciones extracontractuales que puedan surgir en el futuro⁹⁷. Esta circunstancia tiene gran relevancia desde la perspectiva de los daños y la responsabilidad extracontractual derivada del uso de los sistemas de IA, y obligará a los fabricantes y proveedores de servicios a tomar en consideración que los futuros daños derivados de su producto podrían dar lugar a una reclamación de este tipo

⁹³ Convenio de 4 de mayo de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera, *Vid.*, <https://www.hcch.net/es/instruments/conventions/full-text/?cid=81>

⁹⁴ Convenio de 2 de octubre de 1973 sobre Ley Aplicable a la Responsabilidad por Productos, *Vid.*, <https://www.hcch.net/es/instruments/conventions/full-text/?cid=84>

⁹⁵ *Vid.*, el Considerando 6 del Reglamento Roma II.

⁹⁶ *Ibidem*, artículo 1.2 g).

⁹⁷ *Ibidem*, artículo 2, apartados 1 y 2.

que quedaría cubierta por el ámbito de aplicación material del Reglamento Roma II respecto a la ley aplicable.

Asimismo, el Reglamento incluye entre las obligaciones extracontractuales a las que resulta de aplicación aquellas basadas en responsabilidad objetiva⁹⁸, a pesar de que se trata de una categoría no exenta de controversia en las legislaciones de algunos Estados miembros⁹⁹. Sin embargo, este aspecto resulta muy apropiado ante la posible regulación de los daños causados por sistemas de IA en vehículos automatizados que puedan quedar sujetos a responsabilidad objetiva. Y, en estos casos, los fabricantes y proveedores de servicios tendrán que asegurarse de que sus productos son lo suficientemente seguros para no causar un daño y, además, adoptar las medidas pertinentes para mitigar los mismos, por ejemplo, asegurando estos productos.

A su vez, el carácter universal del Reglamento Roma II garantiza que la ley designada por el mismo sea aplicable aun cuando no se trate de la ley de un Estado miembro¹⁰⁰. Aplicación de una ley estatal designada por el Reglamento que solamente podrá excluirse cuando fuere manifiestamente incompatible con el orden público del foro, en cuyo caso, el tribunal competente podría aplicar su propia ley (*lex fori*) y dejar inaplicada la ley designada por el Reglamento Roma II¹⁰¹.

En fin, la exclusión del reenvío facilita la previsibilidad de la ley aplicable y permite mitigar el recurso al *forum shopping*¹⁰². Si bien, como algún autor ha señalado la exclusión del reenvío podría generar la aplicación de leyes diferentes en varios Estados miembros en supuestos de accidentes en los que intervengan vehículos automatizados¹⁰³.

⁹⁸ *Ibidem*, Considerando 15.

⁹⁹ *Vid.* al respecto, CASTRONUOVO, C., *Responsabilità civile*, Giuffrè, Milano, 2018, p. 765; KADNER-GRAZIANO, T., “Les principes du droit européen de la responsabilité délictuelle” (Principles of European Tort Law) - forces et faiblesses, en WINIGER, B., (ed.) *La responsabilité civile européenne de demain. Projets de révision nationaux et principes européens*, Schulthess and Bruylant, Geneva, 2008, p. 219; y KOCH, B. A., “The work of the European group of Tort Law - The case of strict liability”, *The American Journal of Comparative Law*, 2005, p. 189.

¹⁰⁰ Artículo 3 del Reglamento Roma II.

¹⁰¹ *Ibidem*, artículo 26.

¹⁰² *Ibidem*, artículo 24, que excluye el reenvío.

¹⁰³ VON HEIN, J., “Forward to the Past. A Critical Evaluation of the European Parliament’s Approach to Artificial Intelligence in Private International Law”, en Voeneke, S., Kellmeyer, P., Mueller, O., y Burgard, W., (eds), *The Cambridge Handbook of Responsible Artificial Intelligence*, Cambridge University Press, Cambridge, 2022, pp. 215-216, citando el documento del Parlamento Europeo y a KADNER GAZIANO, T., “Cross-border Traffic Accidents in the EU- the Potential Impact of Driverless Cars, European Parliament- Directorate-General for Internal Policies of the Union. Brussels, 2016, pp. 37 y ss., disponible en [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU\(2016\)571362_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf)

A) *Autonomía de la voluntad de las partes y uso de sistemas de IA*

En el ámbito de los accidentes de tráfico transfronterizos, no será muy habitual que las partes hayan pactado la ley aplicable en caso de conflicto. Sin embargo, el Reglamento considera que, “... *para respetar el principio de autonomía de las partes y reforzar la seguridad jurídica, estas deben poder elegir la ley aplicable a una obligación extracontractual*”¹⁰⁴.

Por tanto, la elección de ley es posible previo cumplimiento de alguna de las siguientes condiciones: que se haga con posterioridad al hecho generador del daño, es decir, el accidente¹⁰⁵ -esta norma tiene como finalidad la protección de la parte débil, en este caso, la víctima del accidente-; o que el acuerdo se hubiese negociado libremente antes del hecho generador del daño, para lo que se exige que las partes hubiesen desarrollado previamente o estuviesen desarrollando una actividad comercial¹⁰⁶. Y, en ambos casos, la elección podrá hacerse de manera expresa o resultar de modo implícito de las circunstancias del caso¹⁰⁷.

Pues bien, esta solución que prevé el Reglamento Roma II podría ser muy útil para ciertos contratos relacionados con los vehículos automatizados, porque permitiría a las partes que tienen una relación contractual elegir la ley aplicable incluso para los supuestos de responsabilidad extracontractual derivados de la contractual, aunque no frente a terceros, como las víctimas del accidente. Y, considerando las diferencias existentes entre las legislaciones nacionales respecto a la delimitación entre responsabilidad contractual y no contractual, parece aconsejable que las partes sujetas a una relación contractual pacten, igualmente, la ley aplicable para el supuesto de daños derivados de una no contractual en el ámbito de los siniestros con vehículos automatizados.

Dicho esto, no hay que olvidar que la autonomía de la voluntad de las partes tiene dos limitaciones: en primer lugar, la observancia de las disposiciones de la ley -que no puedan excluirse por acuerdo- del país donde todos los elementos de la situación se encuentren localizados en el momento de producirse el accidente; y, en segundo lugar, las disposiciones del Derecho comunitario que se apliquen en el Estado miembro del foro y no puedan excluirse mediante acuerdo, cuando todos los elementos pertinentes de la situación se encuentren localizados en uno o varios Estados miembros en el momento del accidente¹⁰⁸.

¹⁰⁴ Considerando 31 del Reglamento Roma II.

¹⁰⁵ *Ibidem*, artículo 14. 1 a).

¹⁰⁶ *Ibidem*, artículo 14.1 b).

¹⁰⁷ *Ibidem*, artículo 14.1, párrafo segundo.

¹⁰⁸ *Ibidem*, artículo 14, apartados 2 y 3.

B) Norma general: lex loci damni y accidentes de tráfico transfronterizos con vehículos automatizados

El Reglamento Roma II opta por el tradicional sistema de norma de conflicto bilateral estableciendo como norma general el punto de conexión la ley del país donde se produce el daño (*lex loci commissi delicti*), con independencia del “... país donde se haya producido el hecho generador del daño y cualesquiera que sean el país o los países en que se producen las consecuencias indirectas del hecho en cuestión”¹⁰⁹.

Por consiguiente, en ausencia de normas específicas para regular la responsabilidad extracontractual en materia de accidentes de tráfico transfronterizos, hay que acudir a la regla general que establece como ley aplicable la del país donde se produce el daño, a saber, el lugar de la colisión o accidente, con independencia del país donde se haya producido el hecho generador del daño¹¹⁰. Porque, tanto en la Propuesta de Reglamento cuanto, en sus Considerandos, queda patente que el legislador considera suficiente esta norma general para regular ese tipo de supuestos¹¹¹.

Se trata de una norma de conflicto de leyes tradicional en el Derecho internacional privado, basada en la conexión territorial y sobre la base de la responsabilidad objetiva que se predica neutral, pues no favorece ni al causante del daño ni a la víctima, sino que trata de buscar un justo equilibrio entre los intereses de las partes en litigio¹¹². Además, respeta el interés del Estado en el que tiene lugar el daño, primando el lugar de producción del daño di-

¹⁰⁹ *Ibidem*, artículo 4.1.

¹¹⁰ Respecto al lugar en el que se produce el daño, será de aplicación la doctrina del TJUE elaborada en interpretación del artículo 7.2 del Reglamento Bruselas I bis por la coherencia que se debe garantizar en la aplicación de ambos instrumentos. *Vid.*, en este sentido, el Considerando 7 del Reglamento Roma II.

¹¹¹ *Vid.*, CALVO CARAVACA, A. L., y CARRASCOSA GONZÁLEZ, J., “El Reglamento Roma II. Reglas generales sobre determinación de la ley aplicable a las obligaciones extracontractuales”, *Revista Crítica de Derecho Inmobiliario*, 2009, n° 712, p. 838; y DE MIGUEL ASENSIO, P. A., “El régimen comunitario relativo a la ley aplicable a las obligaciones extracontractuales”, *Revista Española de Seguros*, 2009, n° 140, 2009, párrafo 26.

¹¹² *Vid.*, al respecto, DE MIGUEL ASENSIO, P. A., “El régimen comunitario ...”, *loc. cit.*, párrafo 20; FERNÁNDEZ MASIÁ, E., “Primeras consideraciones sobre el anteproyecto de Reglamento sobre la ley aplicable a las obligaciones extracontractuales (Roma II)”, *Actualidad Civil*, septiembre 2003, n° 34, p. 911; GARCIMARTÍN ALFÉREZ, F. J., “La unificación del derecho conflictual en Europa: El Reglamento sobre la ley aplicable a las obligaciones extracontractuales (Roma II)”, *Diario La Ley*, 2007, n° 6811, p. 9; KADNER GRAZIANO, T., “Le nouveau droit International privé communautaire en matière de responsabilité extracontractuelle”, *Revue critique de droit International privé*, 2008, n° 3, p. 457; y VON HEIN, J., “Chapter II Torts/Delicts” en G. P. Calliess, (ed) *Rome Regulations, commentary on the European rules of the Conflicts of Laws*, The Netherlands, Wolters Kluwer, 2011, p. 402.

recto sin otorgar relevancia al lugar en el que se produzcan las consecuencias indirectas.

La misma norma será de aplicación cuando en un siniestro de carácter internacional intervengan vehículos automatizados. No obstante, en estos casos, la producción del daño en diferentes lugares podría plantear problemas añadidos pues, al contrario de lo que sucede en el ámbito de la competencia judicial internacional, donde la víctima pueda elegir el tribunal competente en función de la regla del principio de ubicuidad desarrollado por el TJUE en su sentencia *Mines de Potasse d'Alsace*, en el ámbito de la ley aplicable esto no es factible.

Y, en estos casos, tal y como señalaba la Comisión Europea en su Propuesta de Reglamento Roma II, cuando se causen daños en varios países procede aplicar de manera distributiva las leyes de todos los países en cuestión¹¹³, de acuerdo con la tesis o regla del mosaico establecida por el TJUE¹¹⁴. No obstante, esta interpretación ha sido criticada por una parte de la doctrina por entender que no aporta certeza y previsibilidad y tampoco contribuye a alcanzar soluciones uniformes¹¹⁵.

Empero, esta norma decaerá en favor de la ley del país en el que la persona cuya responsabilidad se alega y la persona perjudicada tengan su residencia habitual en el momento de producirse el daño -residencia habitual común de las partes-¹¹⁶. Si bien es cierto que en el ámbito de los sistemas de IA aplicados a la conducción de vehículos no será habitual que la fabricación del vehículo se haya llevado a cabo en el mismo país donde tiene la residencia habitual su propietario o usuario. Y lo mismo sucederá con los prestadores de servicios de los componentes digitales instalados en el vehículo.

¹¹³ Vid., la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la ley aplicable a las obligaciones extracontractuales (Roma II), COM (2003) 427 final, de 22.07.2003, p. 12.

¹¹⁴ Sentencia del TJUE, de 7.03.1995, asunto C-68/93 - *Shevill y otros/Presse Alliance*, ECLI:EU:C:1995:61.

¹¹⁵ Vid., por todos, DAVÌ, A., *La responsabilità ...*, op. cit., pp. 47 y ss.; FRANZINA, P., "Il Regolamento n° 864/2007/CE sulla legge applicabile alle obbligazioni extracontrattuali, *Le nuove leggi civili commentate*, CEDAM, Padova, 2008, p. 994; JOUBERT, N., "Les règles de conflit spéciales en matière de délits dans le Règlement du 11 Juillet 2007 (Rome II)", en CORNLOUP, S., y JOUBERT, N., *Le Règlement communautaire Rome II sur la loi applicable aux obligations non contractuelles*, Litec, Paris, 2008, p. 57; y WILSKE, S., "Conflict of laws in cyber torts", *Computer und Recht International*, 2. Jahrg. (2001), 3, p. 68.

¹¹⁶ Artículos 4.2 y 23 del Reglamento Roma II, donde indican que la residencia habitual de las personas físicas que estén ejerciendo su actividad profesional será la del "... establecimiento principal de dicha persona"; y la de una sociedad, asociación o persona jurídica "... el lugar de su administración central". Además, "Cuando el hecho generador del daño o el daño se produzca en el curso de las operaciones de una sucursal, agencia o cualquier otro establecimiento, se considerará residencia habitual el lugar en el que dicha sucursal, agencia u otro establecimiento está situado".

Finalmente, como cláusula de cierre, el Reglamento dispone que, si del conjunto de circunstancias se desprende que el hecho dañoso presenta vínculos manifiestamente más estrechos con otro país, distinto de aquel en el que se haya producido el hecho generador del daño o de aquel en que las partes -víctima y causante del daño- tengan su residencia habitual, se aplicará la ley de este otro país¹¹⁷.

Se trata de una excepción general que trata de corregir el resultado no deseado de aplicar los apartados 1 y 2 antes mencionados, pero que ha de aplicarse de manera excepcional, pues tal y como explicaba la Comisión Europea en su Propuesta de Reglamento introduce cierta incertidumbre en la ley aplicable. De ahí la exigencia de que obligación presente un vínculo “*manifiestamente más estrecho*” con otro país, es decir, el principio de proximidad. En definitiva, permite al juez adaptar la norma rígida a un caso concreto para aplicar la ley que corresponda al centro de gravedad de la situación que ha generado el litigio¹¹⁸.

Al objeto de considerar los vínculos manifiestamente más estrechos con otro país, estos podrían basarse en la existencia de una relación previa entre las partes, por ejemplo, un contrato estrechamente vinculado con el hecho dañoso en cuestión. De este modo, se conciliaría la exigencia de seguridad jurídica y la necesidad de hacer justicia en casos individuales, elementos esenciales en los que se basa la aplicación del Reglamento Roma II¹¹⁹.

Precisamente, la aplicación de esta cláusula de cierre podría suponer la solución a aquellos supuestos en los que los daños se verifiquen en diferentes estados, aplicando la ley del país que presenta los vínculos manifiestamente más estrechos con el litigio en lugar de aplicar de manera distributiva la ley de cada uno de los Estados en los que se ha dejado manifestar el daño pues, tal y como he señalado, esta solución no resulta del todo satisfactoria.

Igualmente, la aplicación de la cláusula de los vínculos manifiestamente más estrechos puede aportar soluciones en aquellos casos en los que se hayan producido daños online, porque en estos casos resultará complejo identificar su correspondencia con un lugar físico. Así, en los daños que puedan derivar-

¹¹⁷ *Ibidem*, artículo 4.3.

¹¹⁸ COM (2003) 427 final, *doc. cit.*, p. 13. Hay que recordar que, hasta la fecha, la interpretación de la cláusula de escape prevista en el artículo 4.3 del Reglamento Roma II no ha sido objeto de interpretación por parte del TJUE. Resulta de gran interés, sin embargo, la interpretación efectuada de este precepto por la *High Court* inglesa en los asuntos *Winrow v. Hemphill* [2014] EWHC 3164 (Queen’s Bench Division) y *Marshall v Pickard* [2015] EWHC 3421 (Queen’s Bench Division). *Vid.*, al respecto, LAFUENTE SÁNCHEZ, R., “Ley aplicable a la responsabilidad derivada de accidentes de circulación por carretera: la cláusula de escape del artículo 4. 3º del Reglamento Roma II a la luz de la jurisprudencia inglesa”, *Anuario Español de Derecho Internacional Privado*, t. XVI, 2016, pp. 463-503.

¹¹⁹ *Vid.*, Considerando 14 del Reglamento Roma II.

se de los sistemas de IA instalados en un vehículo, por ejemplo, el software, esta solución resultará más apropiada considerando que el lugar de fabricación del mismo, el lugar de desarrollo y el lugar de comercialización pueden no coincidir.

C) *Ley aplicable a la responsabilidad por los daños causados por productos defectuosos*

La incorporación de los vehículos automatizados implica que en el ámbito de la responsabilidad extracontractual habrá que prestar mayor atención a todos los aspectos relacionados con la responsabilidad por los daños causados por productos defectuosos. Pensemos que hasta ahora la piedra angular sobre la que se asentaba la responsabilidad en este tipo de siniestros era el factor humano -la culpa o negligencia del conductor-, mientras que con la incorporación de los vehículos automatizados van a entrar en juego otros aspectos de carácter objetivo determinados por la interacción de la tecnología y la IA.

a) El artículo 5 del Reglamento Roma II

En este punto, hay que recordar que la responsabilidad derivada de daños causados por productos defectuosos queda sujeta a normas de conflicto especiales en el propio Reglamento Roma II, que trata de buscar el equilibrio entre la protección de la persona perjudicada, como parte débil, y el interés del fabricante a la hora de determinar la ley aplicable en caso de litigio¹²⁰. Y esta norma de conflicto, se aplicará como alternativa cuando las partes no hayan ejercitado la libertad de elección prevista en el propio Reglamento¹²¹.

Respecto a la redacción de la norma que regula la ley aplicable a la responsabilidad por los daños causados por productos defectuosos, hay que señalar los siguientes aspectos. En primer lugar, el Reglamento no incluye una definición de término “producto”, por lo que hay que remitirse a lo dispuesto en la Directiva 85/374 sobre responsabilidad por los daños causados por productos defectuosos y considerar la limitación de su ámbito de aplicación a

¹²⁰ *Ibidem*, artículo 5 y Considerando 20 donde señala, al respecto de esta norma de conflicto, que “... debe responder a los objetivos que son el justo reparto de los riesgos inherentes a una sociedad moderna caracterizada por un alto grado de técnica, la protección de la salud de los consumidores, el incentivo a la innovación, la garantía de una competencia no falseada y la simplificación de los intercambios comerciales. La creación de un sistema de cascada de factores conexos, combinada con una cláusula de previsibilidad, constituye una solución equilibrada habida cuenta de estos objetivos”.

¹²¹ *Ibidem*, artículo 14.

los bienes muebles¹²², o abogar por una definición más amplia, lo que sería deseable con el fin de incluir en su ámbito de aplicación los productos intangibles como el software que será un elemento importante en el desarrollo de la IA en la conducción automatizada¹²³.

En segundo lugar, aun cuando el mencionado precepto incluye en su título el término “daños causados por productos defectuosos”, en su redacción se refiere a las obligaciones extracontractuales que se deriven del daño causado por un producto, sin distinguir sobre su posible defectuosidad. Considerando, por tanto, una interpretación extensiva, se podría concluir que incluye tanto a los productos defectuosos cuanto a los peligrosos y, en ese sentido, cabe defender la aplicación de estas normas de conflicto a los productos tecnológicos que forman parte de la IA y la conducción automatizada por el potencial riesgo que implican, por ejemplo, el daño causado por el software instalado en un vehículo autónomo¹²⁴.

Por lo que se refiere a los puntos de conexión para determinar la ley aplicable en esta materia, el Reglamento Roma II dispone un sistema en cascada: en primer lugar, la ley del país de la residencia habitual común de la persona cuya responsabilidad se alega y la persona perjudicada (*lex loci domicilii communis*), remitiendo, de este modo, a la norma de conflicto prevista en el artículo 4.2¹²⁵; en segundo lugar, en ausencia de residencia habitual común de las partes, la ley del país de la residencia habitual de la víctima en el momento de producirse el daño si el producto se comercializó en dicho país (regla del *international stream of commerce*)¹²⁶; en su defecto, la ley del país donde se ad-

¹²² Tal y como señalaba la Comisión en su Exposición de motivos de la Propuesta de Reglamento Roma II, COM (2003) 427 final, *doc. cit.*, p. 14. En la doctrina, *Vid.*, entre otros, HUBER, P., e ILLMER, M., “International Product Liability. A Commentary on Article 5 of The Rome II Regulation”, *Yearbook of Private International Law*, vol. 9, 2007, pp. 37-38; y STONE, P., “Product Liability under the Rome II Regulation”, en AHERN, J., y BINCHY, W., (eds.) *The Rome II Regulation on the law applicable to non-contractual obligations: a new international litigation regime*, Leiden Boston, MARTINUS Nijhoff Publishers, 2009, p. 181.

¹²³ *Vid.*, al respecto, PLENDER, R., y WILDERSPIN, M., *The European Private International Law of Obligations*, 3rd ed., London, Sweet & Maxwell, Thomson Reuters, 2009, p. 551; y SWIERCZYNSKI, M., y ŻARNOWIEC, L., “Law applicable to liability for damages due to traffic accidents involving autonomous vehicles”, *Masaryk University Journal of Law and Technology*, vol. 14, 2020, p. 186 disponible en <https://journals.muni.cz/mujlt/article/view/12425>.

¹²⁴ *Vid.*, en este sentido, DICKINSON, A., *The Rome II Regulation: The law applicable to non contractual obligations*, Oxford, Oxford University Press, 2008, p. 370; así como ILLMER, M., “The New European Private International Law of Product Liability-Steering Through Troubled Waters”, *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, *The Rabel Journal of Comparative and International Private Law*, vol. 73, n° 2, 2009, pp. 281-282.

¹²⁵ Artículo 5.1, del Reglamento Roma II, que remite al artículo 4.2.

¹²⁶ *Ibidem*, artículo 5.1 a).

quirió el producto si fue comercializado allí¹²⁷; y, en su defecto, la ley del país donde se produjo el daño, si el producto se comercializó en dicho país¹²⁸.

Esta norma de conflicto -el país donde se produce el daño-, es la regla básica que establece la norma general en su artículo 4; sin embargo, en el ámbito de la responsabilidad por productos defectuosos, ocupa el último lugar en la jerarquía de conexiones previstas en el artículo 5, por lo que se establece una clara distinción entre la responsabilidad no contractual con carácter general y la derivada de los productos defectuosos. Consecuentemente, en el ámbito de los siniestros con vehículos automatizados, esta distinción puede tener una incidencia decisiva, según se califique la responsabilidad como general o derivada de un defecto del vehículo¹²⁹.

Además, hay que indicar que será aplicable la ley del país donde tenga su residencia habitual la persona cuya responsabilidad se alega cuando no pueda prever razonablemente la comercialización del producto o de un producto del mismo tipo en alguno de los países antes mencionados¹³⁰.

Para finalizar, el Reglamento añade el criterio de los vínculos manifiestamente más estrechos al considerar la aplicación de la ley de ese país en detrimento de cualesquiera de las señaladas anteriormente. La vinculación del hecho dañoso con un país debe desprenderse del conjunto de circunstancias del caso y, a título de ejemplo, el Reglamento indica que “... *un vínculo manifiestamente más estrecho con otro país podría estar basado en una relación preexistente entre las partes, como por ejemplo un contrato, que esté estrechamente vinculada con el hecho dañoso en cuestión*”¹³¹. Se trata, por tanto, al igual que sucede con el artículo 4.3 de la norma general, de una cláusula que habrá de aplicarse de manera excepcional considerando el principio de proximidad del hecho dañoso con un determinado país.

b) Responsabilidad por sistemas de IA defectuosos en la conducción automatizada

Respecto a la aplicación de estas normas de conflicto especiales en materia de daños causados por productos defectuosos y, en particular, respecto a los sistemas de IA instalados en vehículos autónomos, pueden plantearse varios problemas.

¹²⁷ *Ibidem*, artículo 5.1 b).

¹²⁸ *Ibidem*, artículo 5.1 c).

¹²⁹ VON HEIN, J., “Forward to the Past. A Critical Evaluation of the European ...”, *loc. cit.*, p. 219.

¹³⁰ Artículo 5.1, último párrafo del Reglamento Roma II.

¹³¹ *Ibidem*, artículo 5.2.

En primer lugar, si bien la determinación de la residencia habitual de la persona perjudicada no presenta grandes problemas, la identificación de la comercialización del producto en ese país puede resultar problemática si consideramos la comercialización de un producto en varios territorios al mismo tiempo -ya sea de forma presencial o virtual- o que, en el caso de los sistemas de IA aplicados a los vehículos automatizados, la actualización del software llevada a cabo de manera online puede considerarse como un producto nuevo diferente al inicialmente comercializado.

En segundo lugar, la determinación del lugar de adquisición del producto donde este hubiese sido comercializado, plantea dificultades similares porque estos pueden adquirirse a distancia y, en ese caso, resulta complicado determinar el lugar físico de adquisición y/o comercialización del mismo.

En tercer lugar, la identificación del país en el que se produjo el daño que, a su vez, fue el de comercialización del producto, vuelve a plantear dificultades cuando se trate de productos que han causado una pluralidad de daños en distintos lugares.

Por lo que respecta a la aplicación del apartado segundo del artículo 5.1, hay que señalar que tampoco será fácilmente aplicable en los daños causados por sistemas de IA en los vehículos automatizados. Obviamente, los fabricantes de estos productos son conscientes de que su distribución online se llevará a cabo en múltiples territorios, por lo que alegar que no pudo prever razonablemente la comercialización del producto o de un producto del mismo tipo en el país cuya ley sea aplicable con arreglo al artículo 5.1, letras a), b) o c), será ciertamente complejo. Para ello, podrán utilizar los instrumentos existentes que les permitan delimitar los mercados donde va a comercializar su producto y excluir aquellos a los que no desea dirigir su actividad.

Por último, cuando en virtud de la aplicación de los artículos 1 y 2 de la Directiva 85/375 sobre productos defectuosos no fuese de aplicación el artículo 5 del Reglamento Roma II, porque los sistemas de IA que han causado el daño no fuesen considerados bienes muebles tangibles, la norma general del artículo 4 entraría en juego con el fin de determinar la ley aplicable si bien, como algunos autores han recordado, los puntos de conexión previstos en el mismo no son tan beneficiosos para la víctima como los previstos en el artículo 5¹³².

D) Reglas especiales

El Reglamento Roma II dispone que las disposiciones del Derecho comunitario que, en materias concretas, regulen los conflictos de leyes relativos a

¹³² *Vid.*, al respecto, ILLMER, M., “The New European Private International Law of Product...”, *loc. cit.*, p. 284.

las obligaciones extracontractuales se aplicarán con carácter preferente sobre las del propio Reglamento¹³³.

En este sentido, pueden citarse, en primer lugar, las normas de conflicto incluidas en el RGPD¹³⁴ que, como se ha puesto de manifiesto en esta obra, pueden tener relevancia en los casos de sistemas de IA aplicados a los vehículos automatizados y la recogida y tratamiento de los datos que estos sistemas lleven a cabo. Asimismo, la Directiva sobre el comercio electrónico, que establece el principio del país de origen o cláusula del mercado único¹³⁵, si bien, el TJUE ya ha manifestado que el artículo 3, apartado 2, de la Directiva “... *no impone una transposición que revista la forma de norma específica de conflicto de leyes*”¹³⁶.

3.2.3 Los Convenios de La Haya

Como es bien sabido, desde su constitución, la Conferencia de La Haya de Derecho Internacional Privado ha desarrollado un papel decisivo en la armonización de las cuestiones de Derecho internacional privado. Aunque en materia de ley aplicable a las obligaciones no contractuales no existe un Convenio de carácter general, el Convenio de 1971 sobre la ley aplicable a los accidentes de tráfico transfronterizos juega un papel esencial en la identificación de la ley aplicable a los supuestos de responsabilidad derivada de accidentes de tráfico transfronterizos junto al Reglamento Roma II. Lo mismo sucederá con el Convenio de 1973 sobre la ley aplicable a la responsabilidad por productos a raíz de la incorporación de los vehículos automatizados¹³⁷.

Ello implica que, ante la ausencia de armonización de las legislaciones de los Estados miembros, la coexistencia del Reglamento Roma II y de los

¹³³ Vid., el artículo 27 del Reglamento Roma II, así como su considerando 35 que establece: “*El presente Reglamento no debe perjudicar la aplicación de otros instrumentos que establezcan disposiciones destinadas a contribuir al correcto funcionamiento del mercado interior, en la medida en que no puedan aplicarse junto con la ley designada por las normas del presente Reglamento*”.

¹³⁴ Vid., el artículo 3, Ámbito territorial, del RGPD.

¹³⁵ Artículo 3, apartados 1 y 2 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DOUE L 178, de 17.07.2000).

¹³⁶ Sentencia del TJUE de 25 octubre 2011, asunto C-509/09, *eDate Advertising y otros*, ECLI:EU:C:2011:685, párrafo 63.

¹³⁷ La preferencia en la aplicación de estos convenios deriva de lo dispuesto en el artículo 28.1 del Reglamento Roma II, Relación con los convenios internacionales existentes, donde dispone: “*El presente Reglamento no afectará a la aplicación de los convenios internacionales en que sean parte uno o más Estados miembros en el momento de la adopción del presente Reglamento y que regulen los conflictos de leyes en materia de obligaciones extracontractuales*”.

Convenios de La Haya de 1971 y 1973 a la hora de determinar la ley aplicable puede favorecer el *forum shopping* y permitir a la víctima la elección del tribunal competente en función de la ley aplicable que resulte más favorable a sus intereses. No cabe duda de que este sistema paralelo no contribuye a alcanzar los objetivos previstos en el Reglamento Roma II, como son la previsibilidad y la seguridad jurídica.

A) *El Convenio de La Haya de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera*

En el ámbito de la Unión Europea, el Convenio de La Haya de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera prevalece sobre la norma general prevista en el artículo 4 del Reglamento Roma II en aquellos países donde el mismo es de aplicación, entre ellos, España¹³⁸. Este Convenio tiene carácter universal, por lo que se aplicará aun cuando la ley designada no sea la de un Estado contratante, y su aplicación no dependerá de ninguna condición de reciprocidad¹³⁹.

Respecto a su ámbito de aplicación material, y en relación a los accidentes causados por vehículos automatizados, hay que indicar que el Convenio de La Haya de 1971 excluye "... la responsabilidad de fabricantes, vendedores y reparadores de vehículos"¹⁴⁰, lo cual no implica que no sea de aplicación a los fabricantes de componentes, como el software que se instale en el vehículo¹⁴¹.

Este Convenio establece como principio básico en su sistema de normas de conflicto la *lex loci delicti*, es decir, la aplicación de la ley interna del Estado en cuyo territorio haya ocurrido el accidente.¹⁴² No obstante, incluye algunas excepciones a este principio en función del número de vehículos implicados en el siniestro.

En primer lugar, cuando en el accidente intervenga un solo vehículo matriculado en un Estado diferente a aquel en el que ocurrió el accidente, se aplicará la ley del Estado de matriculación del vehículo con el fin de determi-

¹³⁸ Actualmente, veintiún Estados son parte de este Convenio, trece de ellos Estados miembros de la Unión Europea: Austria, Bélgica, Croacia, Eslovaquia, Eslovenia, España, Francia, Letonia, Lituania, Luxemburgo, Países Bajos, Polonia y República Checa (en adelante, Convenio de La Haya de 1971). *Vid.*, <https://www.hcch.net/en/instruments/conventions/full-text/?cid=81>

¹³⁹ Artículo 11 del Convenio de La Haya de 1971.

¹⁴⁰ *Ibidem*, Artículo 2.1.

¹⁴¹ Algunos autores consideran difícilmente justificable esta distinción entre fabricantes de vehículos y fabricantes de componentes. *Vid.*, al respecto SWIERCZYNSKI, M., y ŻARNOWIEC, L., "Law applicable to liability...", *loc. cit.*, p. 182.

¹⁴² Artículo 3 del Convenio de La Haya de 1971.

nar la responsabilidad en tres supuestos: respecto del conductor, el poseedor, el propietario o cualquier otra persona que tenga un derecho sobre el vehículo, con independencia de cuál sea su residencia habitual¹⁴³; igualmente, se aplicará la ley del Estado de matriculación del vehículo respecto de las víctimas que viajasen como pasajeras, si tenían su residencia habitual en un Estado distinto de aquel en cuyo territorio haya ocurrido el accidente¹⁴⁴; y respecto de las víctimas que se encontrasen en el lugar del accidente fuera del vehículo, si tenían su residencia habitual en el Estado en que dicho vehículo estuviese matriculado¹⁴⁵.

En segundo lugar, cuando en el accidente se vean implicados dos o más vehículos se aplicará una excepción al principio *lex loci delicti* siempre que esos vehículos estuviesen matriculados en el mismo Estado, siendo de aplicación la ley del Estado de matriculación de los vehículos¹⁴⁶.

En tercer lugar, cuando en el accidente se viesen implicadas -ya sea como responsables o víctimas- una o más personas que se encontrasen fuera del o de los vehículos en el lugar del accidente, la derogación del principio *lex loci delicti* únicamente operará cuando todas esas personas tengan su residencia habitual en el Estado en el cual él o los vehículos estuviesen matriculados¹⁴⁷.

Finalmente, hay que tener en cuenta que cuando se encuentren implicados en el siniestro vehículos no matriculados o matriculados en varios Estados, la norma de conflicto no será la ley del Estado de matriculación sino la ley interna del Estado donde estén habitualmente estacionados. Esta misma regla se aplica en aquellos supuestos en los que ni el propietario, ni el poseedor, ni el conductor del vehículo tuvieron, en el momento de ocurrir el accidente, su residencia habitual en el Estado de matriculación del vehículo¹⁴⁸.

Además de todo lo dicho, hay que mencionar que, aunque el Convenio de La Haya de 1971 no prevé la posibilidad de que las partes puedan elegir la ley aplicable a la controversia, ello no impide que puedan hacerlo con posterioridad al hecho generador del daño al socaire del artículo 14 del Reglamento Roma II. De hacerlo así, la libertad de elección prevalecerá frente a las normas de conflicto previstas en el Convenio de La Haya de 1971¹⁴⁹, aunque la doctrina no es unánime a la hora de considerar si la autonomía de la voluntad

¹⁴³ *Ibidem*, artículo 4 a), párrafo primero.

¹⁴⁴ *Ibidem*, artículo 4 a), párrafo segundo.

¹⁴⁵ *Ibidem*, artículo 4 a), párrafo tercero.

¹⁴⁶ *Ibidem*, artículo 4 b).

¹⁴⁷ *Ibidem*, artículo 4 c).

¹⁴⁸ *Ibidem*, artículo 6.

¹⁴⁹ KADNER GRAZIANO, T., "Cross-border Traffic Accidents ..., *doc. cit.*, p. 27.

permitirá excluir la aplicación del Convenio en favor de la ley estatal elegida por las partes¹⁵⁰.

B) El Convenio de La Haya de 1973 sobre Ley Aplicable a la Responsabilidad por Productos Defectuosos

Algo parecido sucede con la ley aplicable a la responsabilidad derivada de los daños causados por productos defectuosos, donde el Convenio de La Haya de 1973 coexiste y se aplica con carácter preferente al Reglamento Roma II y, en particular, a su artículo 5,¹⁵¹ por los jueces y tribunales de aquellos Estados miembros donde el Convenio se aplica, entre ellos, España¹⁵². Como el Reglamento Roma II y el Convenio de La Haya de 1971, este Convenio tiene carácter universal, por lo que se aplicará aun cuando la legislación aplicable no sea la de un Estado contratante¹⁵³.

El Convenio reviste especial importancia por varios motivos: en primer lugar, porque el Convenio de La Haya de 1971 sobre Ley Aplicable en Materia de Accidentes de Circulación por Carretera excluye la aplicación de sus normas a la responsabilidad de fabricantes, vendedores y reparadores de vehículos; en segundo lugar, porque la armonización legislativa en materia de responsabilidad causada por productos defectuosos solamente se ha producido de manera parcial en la Unión Europea a través de la Directiva 85/374; y, en tercer lugar, porque establece un complejo sistema de normas de conflicto sobre la base de diferentes puntos de conexión que no coinciden con lo previsto en el artículo 5 del Reglamento Roma II donde se regula este mismo aspecto.

Este Convenio, tampoco prevé la autonomía de la voluntad de las partes. Empero, estas podrán elegir la ley aplicable a la controversia con base al artículo 14 del Reglamento Roma II que entraría en juego en esos casos prevaleciendo frente a las normas de conflicto previstas en el Convenio de La Haya de 1973¹⁵⁴.

¹⁵⁰ *Vid.*, al respecto, KADNER GRAZIANO, T., “The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability-Interaction, conflicts and future perspectives”, *Nederlands Internationaal Privaatrecht (NIPR)*, 2008, p. 3 disponible en https://www.biicl.org/files/5200_graziano_27-09-10_biicl_1.pdf

¹⁵¹ El artículo 28 del Reglamento II permite la coexistencia de regímenes diversos que regulen conflictos de leyes en materia de obligaciones extracontractuales.

¹⁵² Actualmente, once Estados son parte de este Convenio, siete de ellos Estados miembros de la Unión Europea: Croacia, Eslovenia, España, Finlandia, Francia, Luxemburgo y Países Bajos (en adelante, Convenio de La Haya de 1973), *Vid.*, <https://www.hcch.net/es/instruments/conventions/full-text/?cid=84>

¹⁵³ Artículo 11 del Convenio de La Haya de 1973.

¹⁵⁴ KADNER GRAZIANO, T., “Cross-border Traffic Accidents...”, *doc. cit.* p. 27.

Por lo que respecta a las normas de conflicto, con carácter general establece como punto de conexión la residencia habitual de la persona perjudicada; así, será de aplicación la ley del Estado donde tenga su residencia habitual la persona directamente perjudicada siempre que se cumpla alguna de las siguientes condiciones: que dicho Estado sea también el Estado en el que se encuentra el establecimiento principal de la persona a quien se le imputa la responsabilidad, o el Estado en cuyo territorio hubiese sido adquirido el producto por la persona directamente perjudicada¹⁵⁵.

De no cumplirse ese requisito, habrá que acudir a la *lex loci damni* ya que el Convenio dispone que será aplicable la ley del Estado en cuyo territorio se haya producido el daño siempre que dicho Estado sea también: el de la residencia habitual de la persona directamente perjudicada; o donde se encuentre el establecimiento principal de la persona a quien se le imputa la responsabilidad; o donde el producto ha sido adquirido por la persona directamente perjudicada¹⁵⁶.

Y, cuando no sean de aplicación las normas de conflicto antes señaladas, la ley aplicable será la del Estado en el que se encuentre el establecimiento principal de la persona a quien se le imputa la responsabilidad, aunque, en este caso, el Convenio permite que el demandante pueda basar su reclamación en el Derecho interno del Estado en cuyo territorio se hubiere producido el daño¹⁵⁷.

3.2.4 Conflictos que plantea la existencia y aplicación de diferentes instrumentos para determinar la ley aplicable

A) *Ausencia de coordinación*

El esquema anterior, pone de manifiesto varias deficiencias; en primer lugar, la ausencia de armonización respecto a las normas de conflicto en esta materia; en segundo lugar, que los puntos de conexión que establecen las normas en vigor en la Unión Europea no son idénticos, por lo que la ley aplicable a un mismo supuesto puede variar dependiendo del tribunal competente y de sus normas de conflicto -ya sea el Reglamento Roma II o los Convenios de La Haya 1971 o La Haya 1973-; en tercer lugar, las consecuencias prácticas

¹⁵⁵ Artículo 5 del Convenio de La Haya de 1973.

¹⁵⁶ *Ibidem*, artículo 4.

¹⁵⁷ *Ibidem* artículo 6, que con esta redacción permite volver a la norma de conflicto prevista en el artículo 4 (*lex loci damni*).

de aplicar diferentes normas para determinar la ley aplicable, como la falta de previsibilidad de soluciones a escala europea; en fin, que se trata de una normativa excesivamente compleja no fácil de entender y de aplicar para las partes que intervienen en un siniestro transfronterizo, incluidos los tribunales y profesionales del derecho.

Además, teniendo en cuenta la ausencia de armonización de los derechos nacionales en materia de responsabilidad extracontractual en aspectos tan relevantes como la indemnización de las víctimas o los plazos de prescripción para presentar una acción ante los tribunales, resulta evidente que las soluciones a un mismo problema pueden ser diferentes dependiendo del tribunal que resulte competente, lo que no favorece la seguridad jurídica ni la previsibilidad y certeza de la solución al caso concreto. Por el contrario, esta situación puede fomentar el *forum shopping*, si bien dentro de las posibilidades de elección del tribunal competente que el propio Reglamento Bruselas I bis ofrece a los litigantes en función de la aplicación del artículo 4 o del artículo 7.2, y del derecho nacional que resultaría aplicable (*law shopping*) como consecuencia de la norma de conflicto aplicada por cada tribunal.

Considerando, pues, que en el ámbito de la conducción automatizada la responsabilidad de los fabricantes va a jugar un papel determinante, no hay que subestimar los problemas que pueden plantear la coexistencia de estos instrumentos y la ausencia de coordinación entre los mismos¹⁵⁸.

Porque la coexistencia del Convenio de La Haya de 1971 y del Reglamento Roma II en el seno de la Unión Europea para determinar la ley aplicable a los accidentes de tráfico transfronterizos ha venido planteando problemas jurídicos importantes. Como ya he señalado, incita a la aplicación del *forum shopping* por parte del demandante que tratará de obtener la aplicación de la ley más favorable a sus intereses seleccionando el foro en función del instrumento que un Estado aplique, ya sea el Convenio o el Reglamento¹⁵⁹.

A mayor abundamiento, el Convenio de La Haya de 1971 también ha planteado dificultades técnicas a los tribunales españoles para el reconocimiento del derecho de otros países signatarios; ha dado lugar a una confusa

¹⁵⁸ Vid., DE BRUYNE, J., VANLEENHOVE, C., "The rise of Self-Driving cars: Is the Private International Law framework for non-contractual obligations posing a bump in the road?", *IALS Student Law Review* 5(1), febrero 2018, p. 26 y KADNER GRAZIANO, K., "Cross-border Traffic Accidents ..., *doc. cit.*, p 51.

¹⁵⁹ BORRÁS, A., "La relation des textes de référence avec les textes internationaux", en FALLON, M., LAGARDE, P. y POILLOT-PERUZETTO, S., (dirs), *La matière civile et commerciale, socle d'un code européen de droit international privé ?*, Dalloz, Paris, 2009, p. 152; ESPINIELLA MENÉNDEZ, A., "Accidentes de circulación por carretera: Del Convenio de La Haya de 4 de mayo de 1971 al Reglamento (CE) N° 864/2007 (Roma II), *Anuario Español de Derecho internacional privado*, t. VII, 2007, pp. 510 a 512 y 529.

aplicación para establecer su jurisdicción cuando se trata de un instrumento para determinar la ley aplicable; o ha generado problemas en cuestiones sobre litispendencia¹⁶⁰.

B) Posibles soluciones

Para paliar estas ineficiencias, la doctrina ya ha ido aportando a lo largo de los últimos años posibles soluciones. Una de ellas, sería la denuncia de estos Convenios por parte de los Estados miembros permitiendo así que sus tribunales aplicasen el Reglamento Roma II que aporta soluciones válidas para las situaciones jurídicas que puedan plantearse en el futuro¹⁶¹. Ello permitiría simplificar el panorama normativo y aplicar de manera generalizada el Reglamento Roma II a estas cuestiones, lo que favorecería una mejor adaptación de la norma comunitaria a cada caso concreto y pondría fin a algunas soluciones complejas que disponen los mencionados Convenios¹⁶².

Al mismo tiempo, podría plantearse la modificación del Reglamento Roma II con el fin de incluir normas de conflicto específicas para determinar la ley aplicable a los accidentes de tráfico transfronterizos, al igual que sucede con la responsabilidad derivada de los daños causados por productos defectuosos regulada en su artículo 5.

Otra posible solución, tal vez menos traumática que no implicaría la denuncia de los Convenios de La Haya, podría ser la unificación de normas de conflicto, introduciendo en el Reglamento Roma II una disposición específica aplicable a los accidentes de tráfico transfronterizos que recoja las mismas normas de conflicto que el Convenio de La Haya de 1971, de tal forma que resulte indiferente en cuanto a su resultado la aplicación de uno u otro instrumento¹⁶³. Y la misma reflexión puede hacerse en relación al artículo 5 del Reglamento Roma II, que determina la ley aplicable a las obligaciones

¹⁶⁰ Vid., BADILLO ARIAS, J. A., “El elemento extranjero en los accidentes de circulación. Funciones del consorcio de compensación de seguros y ofesauto”, *Revista de responsabilidad civil, circulación y seguro*, n° 1, 2014, págs. 18-20.

¹⁶¹ Artículo 20 del Convenio de La Haya de 1971 y artículo 21 del Convenio de La Haya de 1973.

¹⁶² Vid., por todos, DE MIGUEL ASENSIO, P., “El régimen comunitario...”, *loc. cit.*, párrafo 26; ESPINIELLA MENÉNDEZ, A., *Las reclamaciones derivadas de accidentes de circulación por carretera transfronterizos*, Madrid, Instituto de Ciencias del Seguro, Fundación Mapfre, 2010, pp. 24 y 82; FERNÁNDEZ ROZAS, J. C. y SÁNCHEZ LORENZO, S., *Derecho internacional privado*, 8ª ed., Civitas Thomson Reuters, Pamplona, 2015, p. 600; y GARAU JUANEDA, L., “La conveniencia de una denuncia por parte de España del Convenio de La Haya de 1971 sobre responsabilidad civil derivada de los accidentes de circulación”, *Anuario Español de Derecho Internacional Privado*, t. VII, 2007, pp. 503-504.

¹⁶³ SWIERCZYNSKI, M., y ŻARNOWIEC, L., “Law applicable to liability ...”, *loc. cit.*, p. 188.

extracontractual que se derive en caso de daño causado por un producto, y el convenio de La Haya de 1973 que regula de manera específica la ley aplicable a la responsabilidad por productos.

También cabría plantear la modificación del Reglamento Roma II, en particular, la redacción de su artículo 28, a la luz de la cláusula de revisión prevista en el artículo 30 del propio Reglamento, con la finalidad de otorgarle preferencia sobre los Convenios de La Haya de 1971 y 1973 en los casos de accidentes de tráfico y productos defectuosos, si bien ello requeriría la renegociación del ámbito de aplicación del Convenio entre las partes signatarias del mismo¹⁶⁴.

De llegarse a esa solución, podría distinguirse entre aquellos casos en los que las partes litigantes tuviesen su residencia habitual en la Unión Europea -aplicando a esos casos el Reglamento Roma II- y aquellos en los que alguna de las partes tenga su residencia fuera de la Unión -aplicando entonces el Convenio de La Haya de 1971 o el Convenio de La Haya de 1973-¹⁶⁵. Ello implicaría una desconexión parcial de los mencionados Convenios por parte de la Unión Europea que, pese a ello, seguirían aplicándose, por lo que no afectaría negativamente al rol que viene desempeñando dentro de la Conferencia de La Haya.

Por último, una mayor armonización del Derecho material de los Estados miembros en esta materia también favorecería la aplicación de estos instrumentos¹⁶⁶. Baste citar los aspectos relativos al resarcimiento de los daños de las víctimas -donde la Directiva 2009/103 establece únicamente unos importes mínimos para los daños dejando que cada Estado pueda elevar estos importes¹⁶⁷; o los plazos de prescripción para ejercitar una acción ante los tribunales -que vienen regulados en la Directiva 85/374 respecto a las reclamaciones por productos defectuosos-¹⁶⁸, mientras que la prescripción y caducidad de las acciones por responsabilidad extracontractual derivadas de accidentes de

¹⁶⁴ DICKINSON, A., *The Rome II Regulation...*, *op. cit.*, p. 362; KADNER GRAZIANO, T., "Cross-border Traffic Accidents...", *loc. cit.*, pp. 27-28; y NAGY, C. I., "The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with some Room for Forum Shopping - How so?, *Journal of Private International Law*, vol. 6, n° 1, 2010, p. 108, disponible en <https://www.tandfonline.com/doi/pdf/10.1080/17536235.2010.11424374?needAccess=true>

¹⁶⁵ KADNER GRAZIANO, T., "*The Rome II Regulation ...*", *loc. cit.*, pp. 9 y 11; y MALATESTA, A., "The Law Applicable To Traffic Accidents", en A. Malatesta (ed) *The Unification of Choice of Law Rules on Torts and Other Non-Contractual Obligations in Europe* (pp.85-106), Milano, CEDAM, 2006, p. 105.

¹⁶⁶ *Vid.* el documento del Parlamento Europeo, Directorate General for Internal Policies, "Choice of Law for Cross-Border Road Traffic Accidents", Author: PAPETTAS, J., 2012, pp. 5 y 21 a 23, disponible en <https://op.europa.eu/o/opportal-service/download-handler?identifier=512308f6-6d06-11e5-9317-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=>

¹⁶⁷ Artículo 9 de la Directiva 2009/103.

¹⁶⁸ Artículos 10 y 11 de la Directiva 85/374.

tráfico transfronterizos se rigen por las disposiciones nacionales de la ley que resulte aplicable de conformidad con el Reglamento Roma II, el Convenio de La Haya de 1971 o el Convenio de La Haya de 1973¹⁶⁹.

En este sentido, cabe recordar que el Parlamento Europeo en su Resolución de 4 de julio de 2017¹⁷⁰, con recomendaciones destinadas a la Comisión sobre el plazo de prescripción para los accidentes de tráfico, incluía el texto de una propuesta de Directiva donde proponía un estándar mínimo de armonización relativa a la duración, comienzo, suspensión y cómputo de los plazos de prescripción que alcanzaría únicamente a las acciones llevadas a cabo al amparo de la Directiva relativa al seguro de los vehículos automóviles¹⁷¹.

3.2.5 Ventajas de aplicar el Reglamento Roma II frente a los Convenios de La Haya

Resulta evidente que el ámbito material de aplicación del Reglamento Roma II es más amplio que el del Convenio de La Haya de 1971; esto significa que sus normas de conflicto son de aplicación a materias excluidas del Convenio lo que, en el caso de la responsabilidad derivada de los accidentes en los que se vean implicados vehículos autónomos, podría ser de gran utilidad.

Asimismo, la autonomía de la voluntad que prevé el Reglamento Roma II permite a las partes la elección *ex post* de la ley aplicable, opción que, como ya he señalado, no contemplan el Convenio de La Haya de 1971.

Por otra parte, la regla *lex loci damni* prevista en el Reglamento Roma II trata de establecer un equilibrio entre los intereses del responsable del daño y la víctima, al tiempo que encaja perfectamente con el sistema de responsabilidad objetiva (*strict liability*)¹⁷² que prevé la Propuesta de Reglamento presen-

¹⁶⁹ Artículo 15 h) del Reglamento Roma II, artículo 8.8 del Convenio de La Haya de 1971 y artículo 8.9 del Convenio de La Haya de 1973.

¹⁷⁰ Resolución del Parlamento Europeo, de 4 de julio de 2017, con recomendaciones destinadas a la Comisión sobre el plazo de prescripción para los accidentes de tráfico (2015/2087(INL) (DO C 334, de 19.09.2018).

¹⁷¹ Artículo 1 del texto de la Propuesta de Directiva sobre los plazos comunes de prescripción para accidentes de tráfico transfronterizos, disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0206+0+DOC+XML+V0//ES>, en relación con los artículos 18, 24 y 25 de la Directiva 2009/103. *Vid.*, al respecto, LAFUENTE SÁNCHEZ, R., “La armonización de los plazos de prescripción en las reclamaciones derivadas de accidentes de tráfico transfronterizos: una prioridad para facilitar el acceso a la justicia de los ciudadanos en el espacio judicial europeo”, en DOMÍNGUEZ LOZANO, P. y ELVIRA BENAYAS, M. J., (Dir.) *Derecho internacional privado europeo. Diálogos con la práctica*, Titant lo Blanch, Valencia, 2020, pp. 116-117.

¹⁷² El Considerando 16 del Reglamento Roma II dispone: “La conexión con el país donde se produzca el daño directo (*lex loci damni*) crea un justo equilibrio entre los intereses de la persona cuya responsabilidad

tada por la Comisión respecto a la responsabilidad derivada de los sistemas de IA que presenten un alto riesgo¹⁷³, como puede ser el caso de la tecnología aplicada a los vehículos automatizados. Pues, tal y como el TJUE ha declarado “... la aplicación de la ley del lugar en que se ha producido el daño directo participa del objetivo, enunciado en el considerando 16 del Reglamento Roma II, dirigido a garantizar una previsibilidad de la ley aplicable...”¹⁷⁴.

A mayor abundamiento, el punto de conexión de la residencia habitual común de la víctima y el responsable del accidente que regula el Reglamento Roma II, y que prevalece sobre el lugar del accidente -*lex loci damni*-, presenta ventajas indiscutibles, especialmente cuando las dos partes tengan su residencia habitual en el territorio de la Unión Europea porque, en esos casos, la conexión de la residencia habitual común responderá a sus legítimas expectativas. Igualmente, resulta más favorable para las partes que la conexión de lugar de matriculación del vehículo que el Convenio de La Haya de 1971 antepone, bajo determinadas circunstancias, a la aplicación de la *lex loci damni*¹⁷⁵.

Finalmente, la cláusula de escape prevista en el Reglamento Roma II también aporta beneficios a la hora de considerar la ley más estrechamente vinculada con el hecho dañoso, si bien su aplicación ha de hacerse de manera restrictiva y siempre que con ello no se favorezca la ley nacional en detrimento de la ley de un tercer Estado. En definitiva, podría decirse que el Reglamento Roma II aporta mayor previsibilidad y flexibilidad frente a las normas de conflicto que incorpora el Convenio de La Haya de 1971.

Lo mismo cabe decir del Convenio de La Haya de 1973, si bien los problemas que plantea son menores porque únicamente siete Estados de la Unión Europea aplican el mismo con preferencia al Reglamento Roma II y, además, porque la Directiva 85/374 sobre la responsabilidad por productos opera una cierta armonización de los derechos nacionales, por lo que la diferencia entre estas normas no es tan acusada como sucede en el caso de la responsabilidad derivada de los accidentes de tráfico.

Sin olvidar que, en este caso, la inaplicación del Convenio de La Haya de 1973 no plantearía grandes problemas porque el Reglamento Roma II establece su propio sistema de normas de conflicto en esta materia lo que no sucede respecto a los accidentes de tráfico transfronterizos.

se alega y la persona perjudicada, y corresponde también a la concepción moderna del Derecho de responsabilidad civil y al desarrollo de los regímenes de responsabilidad objetiva”.

¹⁷³ Vid., el artículo 4 de la Propuesta de Reglamento sobre responsabilidad en materia de IA

¹⁷⁴ Sentencia del TJUE de 10 de diciembre de 2015, asunto C-350/14, *Florin Lazar*, ECLI:EU:C:2015:802.

¹⁷⁵ KADNER GRAZIANO, T., “Cross-border Traffic Accidents...”, *loc. cit.*, pp. 27 y 55; y NAGY, C. I., “The Rome II Regulation and Traffic...”, *loc. cit.*, p. 107.

4. REFLEXIONES FINALES: IDONEIDAD DE LOS INSTRUMENTOS DE DIPR ACTUALMENTE EN VIGOR PARA REGULAR LAS RECLAMACIONES DERIVADAS DE LA CONDUCCIÓN AUTOMATIZADA

4.1 PARA DETERMINAR LA JURISDICCIÓN DE LOS TRIBUNALES DE LA UE

A la vista del análisis efectuado, podría afirmarse que los foros de competencia previstos en el Reglamento Bruselas I bis -foro general del domicilio del demandado, competencias especiales y competencia en materia de seguros- pueden dar una respuesta adecuada a los problemas que planteen las reclamaciones en materia de responsabilidad no contractual derivada del uso de sistemas de IA aplicados a la conducción automatizada.

Ahora bien, se pueden suscitar los mismos problemas de falta de previsibilidad que hasta ahora se han venido detectando en casos muy concretos, por ejemplo, cuando se trate de demandas contra varios demandados que impliquen la determinación de la jurisdicción de los tribunales de la Unión Europea con arreglo al Reglamento y la de terceros Estados de conformidad con las normas internas de cada Estado.

Asimismo, surgirán dudas cuando el daño sea producto de una actividad realizada online -pensemos en la actualización del software instalado en el vehículo automatizado que se realiza a través de un prestador de servicios de manera virtual-, porque en esos casos identificar el domicilio del proveedor -sede estatutaria, administración central o centro de actividad principal- puede resultar complejo, teniendo en cuenta que el lugar de establecimiento del proveedor del servicio no siempre coincidirá con el lugar del dominio principal de internet a través del cual ofrece el servicio. En tales supuestos, tal y como el TJUE ha declarado, el lugar de establecimiento del servidor, por la incierta ubicación que a veces puede implicar, no podría considerarse el lugar del hecho causal a efectos de la aplicación de las disposiciones del Reglamento Bruselas I bis y, en particular, su artículo 7.2¹⁷⁶

Precisamente, por lo que respecta a la regla de competencia prevista en el artículo 7.2, cuando intervengan vehículos autónomos puede resultar más difícil determinar la parte responsable y el lugar donde se ha producido el hecho generador del daño. Así sucederá cuando se vean implicados el fabricante del software, el proveedor de servicios del software y el fabricante final del ve-

¹⁷⁶ Sentencia del TJUE de 19 de abril de 2012, asunto C-523/10, *Wintersteiger AG*, ECLI:EU:C:2012:220, párrafo 36.

hículo que lleva incorporado el software, en cuyo caso, el lugar de producción el daño será la solución más adecuada.

Por lo tanto, hay que traer a colación la reiterada jurisprudencia del TJUE según la cual:

... en el supuesto de que el lugar donde se sitúe el hecho del que puede derivarse una responsabilidad delictual o cuasidelictual y el lugar en que este hecho haya ocasionado un daño no sean idénticos, la expresión «lugar donde se hubiere producido el hecho dañoso [...] debe entenderse referida, al mismo tiempo, al lugar donde ha sobrevenido el daño y al lugar del hecho causante del mismo, de modo que el demandado puede ser emplazado, a elección del demandante, ante el órgano jurisdiccional de cualquiera de esos dos lugares.¹⁷⁷

Y, de conformidad con la misma, señalar que, en los supuestos de daños causados por un sistema de IA, por ejemplo, por el fallo o la falta de actualización del software, los tribunales competentes podrían ser, a elección de la víctima, tanto los del lugar de producción y comercialización del mismo cuanto los del país en el que se produjo la actualización en el vehículo.

4.2 EN MATERIA DE LEY APLICABLE

En fin, al igual que sucede con los instrumentos de Derecho internacional privado en materia de competencia judicial internacional, hay que señalar que las disposiciones en materia de Derecho aplicable actualmente en vigor deberían bastar para dar una respuesta adecuada a las cuestiones de responsabilidad no contractual derivadas del uso de la IA y, por consiguiente, a los problemas que plantea la determinación de la ley aplicable en materia de responsabilidad extracontractual derivada de los siniestros en los que intervengan vehículos automatizados.

Pese a ello, se impone una mejor coordinación de estos instrumentos, por lo que sería aconsejable acabar con la dispersión que representa la coexistencia del Reglamento Roma II con los Convenios de la Haya de 1971 y 1973, y que las nuevas iniciativas legislativas que se planteen en el seno de la Unión Europea sigan los mismos criterios que establecen los instrumentos antes señalados con el fin de evitar que esa dispersión legislativa pueda hacer más difícil la ya compleja aplicación de estas normas.

¹⁷⁷ Sentencia del TJUE de 16 de julio de 2009, asunto C-189/09, *Zuid-Chemie BV, cit.*, párrafo 23.

BILIOGRAFÍA

- BADILLO ARIAS, J. A., “El elemento extranjero en los accidentes de circulación. Funciones del consorcio de compensación de seguros y ofesauto”, *Revista de responsabilidad civil, circulación y seguro*, n° 1, 2014
- BORRÁS, A., “La relation des textes de référence avec les textes internationaux”, en FALLON, M., LAGARDE, P. y POILLOT-PERUZZETTO, S., (dirs), *La matière civile et commerciale, socle d'un code européen de droit international privé ?*, Dalloz, Paris, 2009
- CALVO CARAVACA, A. L., y CARRASCOSA GONZÁLEZ, J., “El Reglamento Roma II. Reglas generales sobre determinación de la ley aplicable a las obligaciones extracontractuales”, *Revista Crítica de Derecho Inmobiliario*, 2009, n° 712
- CAPPIELLO, B., *AI-systems and non-contractual liability. A european private international law analysis*, Giappichelli Editori, Torino, 2022
- CASTRONUOVO, C., *Responsabilità civile*, Giuffrè, Milano, 2018
- DAVÌ, A., *La responsabilità extracontrattuale*, UTET, Torino, 1997
- DE BRUIN, R., “Autonomous Intelligent Cars on the European Intersection of Liability and Privacy: Regulatory Challenges and the Road Ahead”, *European Journal of Risk Regulation*, vol. 7, n° 3, 2016
- DE BRUYNE J. y WERBROUK, J., “Merging self-driving cars with the law”, *Computer Law & Security Review*, 34, 2018, disponible en <https://daneshyari.com/article/preview/10225866.pdf>
- DE BRUYNE, J., VANLEENHOVE, C., “The rise of Self-Driving cars: Is the Private International Law framework for non-contractual obligations posing a bump in the road?”, *IALS Student Law Review* 5(1), febrero 2018
- DE MIGUEL ASENSIO, P. A., “El régimen comunitario relativo a la ley aplicable a las obligaciones extracontractuales”, *Revista Española de Seguros*, 2009, n° 140, 2009
- DICKINSON, A., *The Rome II Regulation: The law applicable to non contractual obligations*, Oxford, Oxford University Press, 2008
- EBERS, M., “La utilización de agentes electrónicos inteligentes en el tráfico jurídico ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?, *InDret*, 3, Julio 2016, disponible en <https://raco.cat/index.php/InDret/article/download/314400/404514/0>.
- ESPINIELLA MENÉNDEZ, A., “Accidentes de circulación por carretera: Del Convenio de La Haya de 4 de mayo de 1971 al Reglamento (CE) N° 864/2007 (Roma II), *Anuario Español de Derecho internacional privado*, t. VII, 2007
- ESPINIELLA MENÉNDEZ, A., *Las reclamaciones derivadas de accidentes de circulación por carretera transfronterizos*, Madrid, Instituto de Ciencias del Seguro, Fundación Mapfre, 2010
- FERNÁNDEZ MASÍÁ, E., “Primeras consideraciones sobre el anteproyecto de Reglamento sobre la ley aplicable a las obligaciones extracontractuales (Roma II)”, *Actualidad Civil*, septiembre 2003, n° 34

- FERNÁNDEZ ROZAS, J. C. y SÁNCHEZ LORENZO, S., *Derecho internacional privado*, 8ª ed., Civitas Thomson Reuters, Pamplona, 2015
- FRANZINA, P., “Il Regolamento n° 864/2007/CE sulla legge applicabile alle obbligazioni extracontrattuali, *Le nuove leggi civili commentate*, CEDAM, Padova, 2008
- FRANZINA, P., *La giurisdizione in materia contrattuale. L'art. 5 n° 1 del Regolamento n. 44/2001 CE nella prospettiva dell'armonia delle decisioni*, CEDAM, Padova, 2006
- GARAU JUANEDA, L., “La conveniencia de una denuncia por parte de España del Convenio de La Haya de 1971 sobre responsabilidad civil derivada de los accidentes de circulación”, *Anuario Español de Derecho Internacional Privado*, t. VII, 2007
- GARCIMARTÍN ALFÉREZ, F. J., “La unificación del derecho conflictual en Europa: El Reglamento sobre la ley aplicable a las obligaciones extracontractuales (Roma II)”, *Diario La Ley*, 2007, n° 6811
- HORVÁTHY, B., “Autonomous vehicles – Challenges for EU private international law”, *EU Business Law and Digital*, 2019, disponible en http://real.mtak.hu/104981/1/Horvathy_autonomous%20vehicles.pdf
- HUBER, P., e ILLMER, M., “International Product Liability. A Commentary on Article 5 of The Rome II Regulation”, *Yearbook of Private International Law*, vol. 9, 2007
- ILLMER, M., “The New European Private International Law of Product Liability–Steering Through Troubled Waters”, *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, *The Rabel Journal of Comparative and International Private Law*, vol. 73, n° 2, 2009
- JOUBERT, N., “Les règles de conflit spéciales en matière de délits dans le Règlement du 11 Juillet 2007 (Rome II)”, en CORNLOUP, S., y JOUBERT, N., *Le Règlement communautaire Rome II sur la loi applicable aux obligations non contractuelles*, Litec, Paris, 2008
- KADNER GRAZIANO, T., “Le nouveau droit International privé communautaire en matière de responsabilité extracontractuelle”, *Revue critique de droit International privé*, 2008, n° 3
- KADNER GRAZIANO, T., “Cross-border Traffic Accidents in the EU– the Potential Impact of Driverless Cars, European Parliament– Directorate-General for Internal Policies of the Union. Brussels, 2016, disponible en [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU\(2016\)571362_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf)
- KADNER GRAZIANO, T., “The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability–Interaction, conflicts and future perspectives”, *Nederlands Internationaal Privaatrecht (NIPR)*, 2008, disponible en https://www.biicl.org/files/5200_graziano_27-09-10_biicl_1.pdf;
- KADNER-GRAZIANO, T., “Les principes du droit européen de la responsabilité délictuelle” (Principles of European Tort Law) – forces et faiblesses, en WINIGER,

of Law and Technology, vol. 14, 2020, disponible en <https://journals.muni.cz/mujlt/article/view/12425>

- VON HEIN, J., “Chapter II Torts/Delicts” en G. P. Calliess, (ed) *Rome Regulations, commentary on the European rules of the Conflicts of Laws*, The Netherlands, Wolters Kluwer, 2011
- VON HEIN, J., “Forward to the Past. A Critical Evaluation of the European Parliament’s Approach to Artificial Intelligence in Private International Law”, en Voeneky, S., Kellmeyer, P., Mueller, O., y Burgard, W., (eds), *The Cambridge Handbook of Responsible Artificial Intelligence*, Cambridge University Press, Cambridge, 2022
- WILSKE, S., “Conflict of laws in cyber torts”, *Computer und Recht International*, 2. Jahrg. (2001), 3

Vehículos autónomos y responsabilidad civil.

La vacilante ruta marcada por el legislador europeo¹

PEDRO JOSÉ LÓPEZ MAS

*Profesor Ayudante Doctor
Universidad de Alicante*

Sumario: 1. CONSIDERACIONES PRELIMINARES SOBRE LA CONDUCCIÓN AUTOMATIZADA. 1.1. Conceptualización y situación actual. 1.2. Retos jurídicos que presenta este «novedoso» fenómeno. 2. RÉGIMEN JURÍDICO DE LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE VEHÍCULOS A MOTOR, Y BREVES NOTAS SOBRE SU ASEGURAMIENTO. 2.1. Planteamiento de la cuestión. 2.2. El concepto de «vehículo a motor». 2.3. El concepto de «hecho de la circulación». 2.4. El concepto de «conductor». 3. LA INCIDENCIA EN LA CONDUCCIÓN AUTOMATIZADA DE LA NUEVA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL, Y SUS EVIDENTES DISFUNCIONALIDADES. 3.1. Ámbito de aplicación y caracteres. 3.2. Deber de exhibición de pruebas y presunción *iuris tantum* en caso de incumplimiento. 3.3. Presunción *iuris tantum* de la relación de causalidad en caso de culpa. 4 BIBLIOGRAFÍA.

¹ Trabajo realizado al amparo de los Proyectos «La irrupción de la inteligencia artificial en el Derecho de daños y su adaptación a las nuevas tecnologías» - Referencia PID2020-116185GB-I00 (Ministerio de Ciencia e Innovación - Agencia Estatal de investigación) y «La Unión Europea ante los desafíos regulatorios de la Inteligencia Artificial: cuestiones de responsabilidad civil» - CIGE/2023/196 (Conselleria d'Educació, Cultura, Universitats i Ocupació de la Generalitat Valenciana).

1. CONSIDERACIONES PRELIMINARES SOBRE LA CONDUCCIÓN AUTOMATIZADA

1.1. CONCEPTUALIZACIÓN Y SITUACIÓN ACTUAL

No podemos abordar con rigor la responsabilidad civil derivada del manejo de vehículos autónomos -o, según los casos, dotados de cierta autonomía-, y su aseguramiento, sin antes, por un lado, definir el objeto sobre el que girará el presente trabajo y, por el otro, poner el acento en aquellos aspectos que suponen ya, a día de hoy, verdaderos retos para la sociedad desde el punto de vista jurídico.

Si partimos de lo que debemos entender por «conducción automatizada»², comúnmente conocida como autónoma, esta no será sino una actividad en la que, en lugar de una persona (el llamado «operador»), es un sistema de inteligencia artificial (IA, en lo que sigue) el que proporciona las instrucciones al vehículo a motor, a fin de promover su conducción de un punto concreto a otro. Es por ello que, en función del grado de automatización de la conducción, la presencia del operador será más o menos necesaria o relevante³.

A nivel nacional, la Instrucción 15/V-113, de carácter reglamentario, sobre el procedimiento de concesión de autorizaciones para realizar pruebas o ensayos de investigación con vehículos de conducción automatizada, define, a los solos efectos de esta Instrucción, cuándo nos encontramos ante un «vehículo autónomo», estableciendo que será coincidente con «todo vehículo con capacidad motriz equipado con tecnología que permita su manejo o conducción sin precisar la forma activa de control o supervisión de un conductor, tanto si dicha tecnología autónoma estuviera activada o desactivada, de forma permanente o temporal». Asimismo, la citada Instrucción diferencia entre «modo autónomo», describiéndolo como aquella «modalidad de conducción consistente en el manejo o conducción del vehículo autónomo sin el con-

² Nosotros nos inclinamos por el empleo en el presente trabajo de la locución «conducción automatizada», rehusando, en aras de evitar malentendidos y falsas creencias, la expresión «vehículo autónomo», toda vez que bajo su dicción se encierra un error de concepto al hacerse alusión a un proceso que afecta al vehículo en su conjunto, y no solo a la conducción. En este sentido, no es dable afirmar que el vehículo es el que se automatiza, sino, muy al contrario, la conducción, a través de sistemas o *softwares* que la promueven en mayor o menor medida. Así, ZORNOZA SOMOLINOS (2021, 35) explica que «puede haber vehículos convencionales con sistemas que automatizan [...] la conducción [...], y pueden existir vehículos que nacen directamente con sistemas de alta o plena automatización en los que el operador llega a ser prescindible».

³ *Ibid.* (2021, 35).

trol activo de un conductor cuando su tecnología autónoma está activada», y «modo convencional», como «modalidad de conducción de un vehículo autónomo en la que la tecnología autónoma está desactivada y su conducción o manejo debe efectuarse mediante el control activo de un conductor».

Por su parte, el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, (Reglamento 2019/2144, en adelante), en su art. 3, consciente del avance de la técnica en esta materia, aprovecha la ocasión para proporcionar una definición de «vehículo automatizado», en contraposición a «vehículo totalmente automatizado»⁴. La norma comunitaria conceptualiza el primero como aquel «vehículo de motor diseñado y construido para desplazarse de manera autónoma durante determinados períodos de tiempo sin supervisión continuada por parte del conductor pero respecto del cual se sigue esperando o necesitando la intervención del conductor». En cambio, el vehículo totalmente automatizado, según el Reglamento, será aquel «vehículo de motor diseñado y construido para desplazarse de manera autónoma sin supervisión por parte del conductor».

Esta distinción no es baladí, por cuanto la delimitación entre una conducción completamente automatizada y otra en la que tan solo exista una asistencia por parte de uno o varios sistemas de IA tendrá relevancia en el plano jurídico, al tiempo de imputar la responsabilidad derivada de un evento dañoso producido⁵.

Así, pese a lo novedoso de la cuestión a nivel legislativo, tal y como se verá más adelante, los vehículos sin conductor humano -y más aún aquellos que

⁴ Destaca cómo el Reglamento rechaza el uso de la expresión «vehículo autónomo» y, en su lugar, opta por la de «vehículo -conducción- automatizado», por cuanto el uso de aquella acepción es más propio de medios divulgativos, que de una normativa de carácter técnico como la que integra el Reglamento 2019/2144.

⁵ En efecto, el grado de automatización del vehículo adquirirá verdadera trascendencia práctica en tema de responsabilidad civil, toda vez que, para el caso de que ocurra un accidente del cual se derivara la producción de daños, personales, materiales o incluso morales, el modelo de conducción podrá suponer, según el supuesto, que quien respondiera de ellos fuera el fabricante del vehículo, el de los equipos tecnológicos que este tuviera instalados, o incluso el conductor, en atención a la concurrencia que haya podido tener en la conducción y, por ende, en el origen del siniestro. Sobre ello nos pronunciaremos con más detalle *infra*.

Por su parte, ARROYO APARICIO (2022, 130 y 132), en la misma línea, asume que la distinción entre una conducción plenamente autónoma y otra en la que tan solo se plantea una asistencia por parte de uno o varios sistemas inteligentes ha de tener relevancia en el plano jurídico, sobre todo, en lo que respecta a la reclamación de responsabilidad a unos u otros sujetos o a varios de ellos de presentarse una concurrencia de culpas.

tienen incorporadas tecnologías de *Advanced Driver Assistance System* (ADAS, en lo que sigue)⁶- cuentan con cierta presencia desde hace ya algún tiempo. Estos, en atención a su nivel de autonomía, han sido clasificados conforme a distintos modelos que regulan el grado de automatización. Sin embargo, parece que el que mayor acogida e implantación ha tenido es el estándar J3016 (EJ3016, en adelante)⁷, publicado por la *Society of Automotive Engineers* (SAE, en lo sucesivo) en el año 2014 y actualizado en el 2018⁸.

El EJ3016 construye una clasificación basada en seis categorías o niveles de automatización de la conducción, tomando como referencia para determinar el grado de autonomía la atención e intervención que se requiera por parte del conductor, las cuales vendrán determinadas, a su vez, por el movimiento del vehículo, la monitorización del entorno, la capacidad del sistema para afrontar el manejo, así como la conducción del respaldo⁹.

Siguiendo el citado estándar, los niveles de automatización pueden describirse del siguiente modo:

- *Nivel 0 – Sin automatización*: En este nivel es el conductor quien ejecuta todas las tareas relativas a la conducción y, además, de manera manual. A pesar de lo antedicho, ello no obsta para que el coche en cuestión disponga de algún sistema de alerta concreto. Nos encontramos, pues, ante vehículos convencionales.

⁶ Cuando nos referimos a *Advanced Driver Assistance System* aludimos a aquellos sistemas o tecnologías incorporadas a los vehículos que, como indica ZORNOZA SOMOLINOS (2021, 37), «monitorean la conducción y emplean técnicas de visión artificial para recopilar información y ayudar al conductor humano en su tarea». Ejemplos de estos sistemas son los de frenado autónomo de emergencia, alerta de cambio de carril involuntario, detección de somnolencia y fatiga, o reconocimiento de señales de tráfico, entre otros.

⁷ Lo ponen de manifiesto ELIZALDE SALAZAR (2022, 29 y ss.); y ZORNOZA SOMOLINOS (2021, 37 y ss.).

Este último autor critica que no se cuente hasta el momento con un único baremo a seguir en esta materia, coexistiendo varios modelos de niveles de automatización, lo que se traduce en una dispersión de criterios contraria a la seguridad jurídica. Ello es lo que ha tratado de paliar la SAE con el estándar J3016, gracias al papel armonizador que asume. (2021, 38).

⁸ De hecho, tan es así que la propia Instrucción 15/V-113 que comentábamos anteriormente toma como referencia la escala creada por la SAE. *Vid.* p. 6 de la Instrucción.

⁹ En cuanto a los elementos reseñados en el cuerpo de este trabajo, para una mejor comprensión, es importante destacar los siguientes extremos. En primer lugar, el movimiento del vehículo puede ser de dos tipos: longitudinal (acelerar y frenar) y lateral (dirección lateral). En segundo lugar, la monitorización del entorno se refiere a la detección de objetos, a su clasificación y a la reacción frente a los mismos. En tercer lugar, las condiciones de funcionamiento del sistema aluden a las condiciones de visibilidad o localización geográfica del vehículo (como, por ejemplo, a limitaciones temporales, velocidad, tráfico rodado o estado de la vía). Y, por último, la llamada conducción de respaldo incide sobre la necesaria presencia de un sujeto que sea quien supervise y recupere el control de la máquina ante un eventual fallo del sistema. Se hace eco de ello TORROBA DÍAZ (2019, 11-12).

- *Nivel 1 – Asistencia al conductor:* El grado de automatización en este nivel viene reflejado por la incorporación de ADAS, que facilitan al conductor algunas de las tareas, como puede ser el mantenimiento en carril mediante determinados sensores integrados en el vehículo, así como el control de velocidad.
- *Nivel 2 – Automatización parcial:* Si bien el sistema, en este caso, admite mayores ayudas o funcionalidades a la conducción que, de forma puntual, permiten al conductor liberar los pedales o el volante, el vehículo como tal no tiene capacidad suficiente para tomar por sí solo decisiones.
- *Nivel 3 – Automatización condicionada:* En este grado, el vehículo puede asumir funciones de monitorización del entorno y toma de decisiones en lo que respecta a la conducción, aunque, eso sí, en medios controlados. Aquí, el conductor humano deberá estar preparado para intervenir de ser necesario, pero sin que este sea coincidente con la figura tradicional de conductor tal y como la venimos conociendo, en el bien entendido de que haya de tener una atención completa del manejo.
- *Nivel 4 – Alta automatización:* El vehículo realiza todo lo necesario para promover la conducción sin requerir la atención del conductor humano, de modo que, de apreciarse riesgo, el sistema, por sí solo, podrá detener o desplazar el coche a un lugar seguro. Sea como fuere, en este nivel, el conductor seguirá siendo necesario cuando dicho sistema no disponga de toda la información como para continuar de manera autónoma –por carecer de datos del vial ante una modificación de su curso por la ejecución de ciertas obras de remodelación, por ejemplo–.
- *Nivel 5 – Automatización completa:* El sistema desarrolla cualquier tarea de conducción con independencia de las circunstancias de la vía, convirtiéndose el conductor en un mero pasajero, que tan solo ostentará la función de poner en marcha el vehículo y seleccionar el lugar de destino o la ruta.

Considerando los distintos niveles planteados, parece evidente que la conducción plenamente autónoma se identificará con los dos últimos grados expuestos. Y es que es en ellos donde podemos prescindir del factor humano. Ello, sin lugar a duda, obligará a repensar el sistema de responsabilidad y su aseguramiento- al desaparecer irremediamente el concepto de conducción e incidir en el criterio de imputación que tomamos como válido hoy en día en la circulación de vehículos a motor¹⁰.

¹⁰ A la cuestión de si el actual sistema normativo que regula la responsabilidad civil en el marco de la automoción ofrece respuestas válidas a estos nuevos interrogantes que suscita la conducción

1.2. RETOS JURÍDICOS QUE PRESENTA ESTE «NOVEDOSO» FENÓMENO

La entrada del vehículo automatizado en el mercado permite vislumbrar, a poco que reflexionemos, numerosos beneficios para la sociedad en su conjunto, destacando la reducción de la siniestralidad en las carreteras¹¹, que no su eliminación¹²; el ahorro en tiempo y coste económico, aumentando, pues, la productividad de las personas y configurando este medio de transporte como uno más limpio y eficiente¹³; o la desaparición de barreras, en ocasiones infranqueables, a que se tienen que enfrentar determinados colectivos sociales, a los que se les impide por motivos varios la obtención de la correspondiente licencia administrativa para conducir¹⁴. Pero también se plantean retos que no debemos desconocer. Por poner algún ejemplo cercano, la conectividad de los vehículos supondrá un incremento del riesgo de sufrir ataques informáticos o cibernéticos que pretendan el acceso a los datos que estos alberguen, o tengan por fin modificar el *software* en aquellos instalado¹⁵. De igual modo, surgen debates morales en torno a la decisión que ha de tomar el vehículo de hallarse en un escenario en el que necesariamente haya de producir un daño personal a un tercero y, en él, tengamos a dos posibles víctimas¹⁶.

automatizada, le dedicaremos nuestra atención *infra*, por lo que ahora simplemente dejamos planteada la duda para su posterior resolución.

¹¹ Tal y como acertadamente expone NÚÑEZ ZORRILLA (2023, 804), «el error del conductor es la razón principal detrás de más del 90% de todos los accidentes», e incluso cuando el accidente se atribuye al vehículo, carretera o entorno, existen factores humanos adicionales (*v. gr.* falta de atención, distracción o exceso de velocidad).

¹² Piénsese en que la conducción autónoma tenderá a evitar accidentes derivados de la fatiga o la distracción al volante, por cuanto se prescindirá del elemento que las padece, esto es, el ser humano. En este sentido, la automatización de la conducción contribuirá a reducir el número de víctimas mortales y/o heridos graves en carretera, ya que se calcula que más del noventa por ciento de los accidentes de tráfico se debe a errores humanos. Así lo reconoce explícitamente el Reglamento 2019/2144 en su Considerando 23.

Por su parte, en España, la Dirección General de Tráfico (DGT, en lo que sigue) anualmente publica el número de accidentes con víctimas mortales y heridas graves que tienen causa en la circulación por carretera, cifrándolo para el 2023 en 1.145 personas fallecidas y 4.495 que sufrieron heridas de alta consideración.

Al margen de lo anterior, los siniestros derivados de fallos mecánicos del automóvil o de defectos en la configuración o diseño de alguno de los sistemas que el mismo incorpore, sin duda, seguirán produciéndose y con ellos daños eventuales que habrá que atender.

¹³ ELIZALDE SALAZAR (2022, 44).

¹⁴ Por ejemplo, por no reunir las aptitudes psicofísicas requeridas por la legislación vigente al estar aquejada la persona de algún tipo de anomalía física, psíquica o sensorial, o simplemente ser una persona de edad avanzada; o por no tener cumplida la edad legal requerida para la obtención del permiso o licencia.

¹⁵ MARTÍN CASALS (2023, 67).

¹⁶ Algunos autores vienen aseverando que un sistema de IA no puede adoptar decisiones desde el prisma moral, sino que estas son un reducto del que únicamente puede hacer uso el ser humano. LIN; JENKINS; ABNEY (2017); o LIN, P. (2016, 69-85), entre otros.

Y, por supuesto, la complejidad de adaptación de los distintos sistemas legales no solo en el ámbito administrativo en cuanto a la regulación de las obligaciones de los conductores o las prohibiciones en la actualidad vigentes¹⁷, sino también en lo que se refiere al régimen de responsabilidad por daños causados por estos sistemas y su aseguramiento.

Con todo, en estos momentos, según expondremos, parece que lo que más preocupa a las instancias europeas desde el prisma legislativo es la potencialidad dañina de estos vehículos y la falta de seguridad que transmiten al conjunto de la sociedad, a causa del estado incipiente en que, por ahora, se halla la técnica.

Este efecto indeseado no es infundado, habida cuenta del relevante número de accidentes mortales provocado por fallos del sistema de automatización del vehículo y, las más veces, por errores humanos ante una evidente falta de diligencia al tiempo de supervisar y verificar su funcionamiento. Veamos algunos de los ejemplos más sonados al respecto¹⁸.

En el año 2016, se produjo un accidente mortal como consecuencia de la conducción de un Tesla Model S, de nivel 2 SAE, en Florida (Estados Unidos) con el modo semiautomático activado (*Autopilot*). Tras la oportuna investigación, se concluyó que el conductor había desoído las indicaciones del sistema que le advertían de la necesidad de tomar el control manual del automóvil, debido al fallo que había sufrido por un deslumbramiento atribuible al chófer de un camión que no había respetado las normas de incorporación a la vía¹⁹.

¹⁷ Al respecto, surgen dudas tales como si las normas reglamentarias que prohíben al conductor de un vehículo a motor circular con una tasa de alcohol en sangre superior a 0,5 gramos por litro, o de alcohol en aire espirado superior a 0,25 miligramos por litro, del art. 20 del Real Decreto 1428/2003, de 21 de noviembre, por el que se aprueba el Reglamento General de Circulación para la aplicación y desarrollo del texto articulado de la Ley sobre tráfico, circulación de vehículos a motor y seguridad vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo, (Reglamento General de Circulación, en lo sucesivo), deberán seguir estando en vigor, o por el contrario la automatización de la conducción aconsejará una derogación de las mismas.

Otro tanto ocurre con la prohibición de circular a quienes hayan ingerido sustancias psicotrópicas, estimulantes u otras análogas, bajo cuyo efecto se altere el estado físico o mental apropiado para circular del conductor, del art. 27 Reglamento General de Circulación.

E incluso las velocidades máximas y mínimas fijadas para todo tipo de vías, de los arts. 45 y ss. del reseñado texto legal, por cuanto, con la automatización, parece que la siniestralidad, como se apuntaba, descenderá, lo cual permitirá lograr una mayor eficiencia al tiempo de circular con un vehículo a motor.

¹⁸ Ciertos ejemplos incluidos en el cuerpo del presente los detalla BELÓN LAURÍN (2022, 7 y ss.).

¹⁹ Posteriores accidentes con resultado de muerte para el conductor, ocupante, ciclista, motociclista o peatón en los que un vehículo Tesla se ha visto implicado pueden consultarse en la web <https://www.tesladeaths.com/>, donde se realiza, a partir de la información obtenida a través de distintas fuentes periodísticas y/o declaraciones oficiales, una estadística del número de muertes relacionadas

En el año 2018, la compañía UBER desarrolló un vehículo nivel 4 SAE, en concreto, un Volvo XC90, provisto de ADAS, aunque modificado para que estos se desactivaran cuando entrara en modo automatizado. El automóvil funcionaba en carreteras abiertas al tráfico, pero siempre con un conductor de respaldo en su interior y en recorridos preestablecidos, de los cuales el sistema disponía de plena información. Pues bien, en marzo de ese año, uno de los vehículos modificados atropelló mortalmente en Arizona a un peatón que portaba una bicicleta consigo cuando, en plena oscuridad, sin elemento reflectante alguno y encontrándose en una zona no habilitada para el paso, atravesó la calle por la que aquel circulaba. En este caso, los informes de la Junta Nacional de Seguridad del Transporte de Estados Unidos (NTSB) determinaron que el sistema no había evidenciado fallo alguno, siendo imputable el accidente, en realidad, a los elementos por nosotros descritos y que dependían del propio peatón. Así y todo, es importante destacar que la alteración de los componentes del Volvo XC90 respondía a la puesta en marcha del negocio de Vehículo de Transporte con Conductor (VTC), que finalmente se frustró, a resultas del impacto mediático que adquirió la noticia en los medios de comunicación.

Apenas días más tarde de este suceso, se registró un nuevo siniestro en el que se vio implicado un Tesla Model X, nivel 2 SAE, que impactó violentamente contra una barrera central de una intersección ubicada en California, con resultado de muerte para el conductor, que circulaba con el *Autopilot* encendido y sin supervisar la marcha.

Por último, en el año 2021, en California, fue también notorio el accidente mortal de un conductor de un Tesla Model 3, que colisionó contra un camión que había volcado en la autopista. Al parecer, la víctima había publicado días antes del fatal choque un vídeo en una conocida red social en el que se le veía en el asiento del conductor sin las manos en el volante, ni los pies en los pedales, mientras el vehículo avanzaba por la autopista. Las autoridades barajaron la distracción como causa probable del suceso.

Por todo ello, a nuestro juicio, debe abogarse por una evolución responsable de la tecnología, en aras de promover el progreso de la sociedad, reducir las altas tasas de siniestralidad vial y, al mismo tiempo, contribuir al desarrollo de un mundo mucho más verde y limpio, aunque ello siempre habrá de ir acompañado de una regulación garantista, en torno a la homologación

con siniestros derivados de la utilización de vehículos fabricados por la compañía de Elon Musk. A fecha 7 de julio de 2024, el total de muertes recopiladas por el citado portal asciende a 555.

Por otra parte, es también interesante el estudio de las tasas de mortalidad de conductores por marca y modelo al margen de los automóviles Tesla que se lleva a término en <https://www.iihs.org/ratings/driver-death-rates-by-make-and-model/>, que recomendamos al lector visitar.

de los distintos sistemas que se incorporen a los vehículos y, como no podía ser de otro modo, en cuanto a la eventual responsabilidad que pudiera surgir como consecuencia de la producción de un accidente mediando cierto grado de automatización.

2. RÉGIMEN JURÍDICO DE LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE VEHÍCULOS A MOTOR, Y BREVES NOTAS SOBRE SU ASEGURAMIENTO

2.1. PLANTEAMIENTO DE LA CUESTIÓN

En España, la responsabilidad civil derivada de la circulación de vehículos a motor se encuentra regulada en el Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, (TRLRCSVM, en adelante), que sufrió una reforma de calado en el año 2015 por la Ley 35/2015, de 22 de septiembre. Esta última norma introdujo un pionero sistema tabular que tenía por fin valorar los daños sufridos por las personas en accidentes de circulación de la forma más cercana al respeto del principio de la *restitutio in integrum*, tan denostado en la práctica del Derecho de Daños²⁰.

El Texto Refundido hace responsable al conductor, en virtud del riesgo creado por la conducción de un vehículo a motor, de los daños causados a las personas o a los bienes con motivo de la circulación *ex* art. 1. Ya de entrada, la norma liga indisolublemente al conductor con el vehículo a motor manejado, de modo que el primero habrá de asumir la reparación de los daños y perjuicios que se irroguen a terceros, a resultas de su conducción, por el riesgo que la misma entraña²¹.

²⁰ Aunque si bien es cierto que el llamado baremo de tráfico permite reducir la inseguridad jurídica a la hora de proceder a la cuantificación de los daños producidos en accidentes de circulación por carretera, y, en particular, aquellos de corte moral, que son, por su propia naturaleza, difícilmente estimables, no lo es menos que con su aplicación resulta imposible reparar íntegramente el perjuicio padecido. Así, la víctima o perjudicado han de ser colocados en la situación más exacta que hubieran ocupado de no haber sufrido el evento dañoso, pero ello, con el baremo vigente, sin dejar a un lado ni olvidar todas sus bondades, no deja de convertir el Derecho de Daños, sobre todo en el ámbito de la circulación de vehículos a motor, en una idea utópica cuasi platónica en lo que se refiere a la reparación del perjuicio causado.

²¹ En este sentido se pronuncian ZORNOZA SOMOLINOS, A. (2021, 117 y ss.); ARROYO APARICIO (2022, 134 y ss.); y TORROBA DÍAZ (2019, 15 y ss.).

Sin embargo, a continuación, el precepto aclara dos aspectos verdaderamente significativos en relación con el criterio de imputación y la eventual exoneración de responsabilidad del conductor. En efecto, por un lado, de provocarse el daño a bienes personales, según la norma, solo se exonerará de responsabilidad al conductor cuando esta naciera, en exclusiva, por la intervención culposa de la víctima o perjudicado, o cuando tuviera origen por fuerza mayor «extraña a la conducción o al funcionamiento del vehículo», no considerándose tal «los defectos del vehículo ni la rotura o fallo de alguna de su piezas o mecanismos». Por el otro lado, en caso de daños a bienes patrimoniales, el conductor, cómo no, también responderá, si bien a través del sistema de responsabilidad civil clásico, a saber, conforme a lo dispuesto en el art. 1902 y ss. del Código civil, (CC, en lo que sigue) para la responsabilidad civil extracontractual pura, y en el art. 109 y ss. del Código Penal, (CP, en lo sucesivo) para la responsabilidad civil *ex delicto*.

Del análisis del contenido del citado artículo se desprende la asunción por el legislador de un diferente criterio de imputación, en función de si el daño se causa a una persona o, por el contrario, a un bien material. En el primer supuesto, en virtud del riesgo creado por la conducción y por la especial protección que merece el derecho a la vida y a la integridad física, el conductor responderá objetivamente, con independencia de la existencia de culpa, negligencia o dolo que le pudiera ser imputable²². En el segundo, tan solo lo hará de apreciarse el reseñado elemento subjetivo que, con carácter general, como se sabe, es preceptivo en el marco de la responsabilidad civil extracontractual por mor de lo establecido en el art. 1902 CC²³.

²² Lo ponía de manifiesto SOTO NIETO (1989, 25) hace algún tiempo al reconocer que la responsabilidad civil del conductor es objetiva cuando los daños los sufre una persona, por cuanto la ley no exige culpa alguna para hacer nacer la obligación de reparar el perjuicio irrogado a un tercero, y la responsabilidad surge, simple y llanamente, del riesgo.

²³ ARROYO APARICIO (2022, 134-135) entiende que la responsabilidad derivada del daño a las personas debe ser clasificada como cuasi objetiva, por razón del riesgo creado por la conducción del vehículo. En cambio, para el caso de daños en los bienes, el conductor respondería conforme a las normas generales de responsabilidad extracontractual.

A nuestro juicio, no teniendo reparos en aceptar la tesis que asume la autora en lo que respecta a la responsabilidad por la causación de daños en bienes patrimoniales, sí que mostramos nuestra disconformidad con la calificación de la responsabilidad cuando quien padece un perjuicio es un bien de corte personal. Y es que, para nosotros, la responsabilidad por riesgo no ha de emplearse como término sinónimo de responsabilidad cuasi objetiva, toda vez que esta última lo que encierra en su concepto no es más que un problema de *onus probandi*, a saber, de quién es el sujeto que ha de soportar la carga de la prueba. En efecto, a modo de ejemplo, la responsabilidad del empresario del art. 1903.V CC dimana del riesgo que entraña el ejercicio de dicha actividad, pero, no obstante, el Código la tacha de subjetiva -o por culpa-, y, al mismo tiempo, exige al empresario que para liberarse de ella acredite haber obrado con la diligencia de un buen padre de familia. Así, el párrafo séptimo del precepto señala que «La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para preve-

Junto con la anterior regulación, en materia de seguro de responsabilidad civil, hemos de referirnos al Real Decreto 1507/2008, de 12 de septiembre, por el que se aprueba el Reglamento del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor, (RSOA, desde ahora). Y es que, precisamente por la finalidad tuitiva de las normas en materia de responsabilidad civil en la circulación de vehículos a motor, se impone al propietario, como obligación, la suscripción de un seguro que cubra los daños, tanto a personas como a bienes, con motivo de dicha circulación.

Tales normas traen causa de la transposición al ordenamiento jurídico español de la Directiva 2009/103/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como el control de la obligación de asegurar esta responsabilidad (Directiva 2009/103/CE, a partir de este momento). En este sentido, la Directiva no incide sobre los criterios de imputación a los que alude expresamente el TRLRCSVM, ni sobre la regulación pormenorizada del seguro de responsabilidad civil, cosa que sí que hace el RSOA, sino que, muy al contrario, contiene, como suele ser habitual, preceptos de mínimos²⁴. Ello ha dado lugar a tantas normas como Estados miembros coexisten en el seno de la Unión Europea, de ahí que el Tribunal de Justicia de la Unión Europea (TJUE, en adelante) haya tenido que pronunciarse, a través de diferentes cuestiones prejudiciales planteadas por estos últi-

nir el daño», sin perjuicio de repetir frente a sus dependientes lo satisfecho en concepto de daño *ex* art. 1904.I del mismo *corpus* legal.

Por ende, responsabilidad por riesgo no debe confundirse con el carácter objetivo o subjetivo que pudiera ostentar la meritada responsabilidad.

Representa la doctrina del riesgo la notoria STS, Sala de lo Civil, núm. 185/2016, de 18 de marzo, (RJ 2016/983), identificada por todos como «caso Macumba», en la que el Alto Tribunal razonó ante un supuesto en el que un cliente de una sala de fiestas había sufrido un corte en uno de sus pies tras pisar un vaso de cristal roto que estaba en el suelo del local, que es patente la imposibilidad de eliminar por completo el riesgo a sufrir un evento dañoso como el padecido, pero no lo es reducirlo tomando medidas específicamente dirigidas al efecto. Es por ello que la responsabilidad para el empresario derivó no tanto de la objetivación de la responsabilidad, como de no desplegar toda la diligencia que le era exigible en aras de minimizar los riesgos de que los asistentes sufrieran un percance como el que ocurrió en autos.

Como nosotros, REGLERO CAMPOS (2014, 1600 y ss.) acepta que la responsabilidad en la circulación de vehículos a motor es objetiva y el riesgo provoca que el que lo controla responda «de forma prácticamente objetiva», pero sin llegar a ello necesariamente, a menos que la norma se exprese de un modo contrario.

²⁴ En otras palabras, suele ser frecuente que las normas comunitarias, principalmente las Directivas, regulen el contenido mínimo y esencial de la cuestión armonizada a nivel europeo, y dejen un amplio margen de maniobra a la actuación de los distintos Estados miembros, al tiempo de establecer normativas más estrictas que las allí estipuladas. De hecho, el art. 288 del Tratado de Funcionamiento de la Unión Europea (TFUE, en adelante) declara que: «La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios».

mos, acerca de dudas interpretativas que han ido surgiendo con ocasión de la resolución judicial de casos concretos²⁵.

Mención aparte merece la Directiva (UE) 2021/2118 del Parlamento Europeo y del Consejo de 24 de noviembre de 2021 por la que se modifica la Directiva 2009/103/CE, (Directiva 2021/2118, en lo sucesivo), la cual debió haber sido transpuesta a nuestro ordenamiento, a más tardar, el pasado 23 de diciembre de 2023. La misma parte de la premisa de que se han logrado los objetivos pretendidos por la norma del año 2009, lo que aconseja retocar tan solo ciertos aspectos de ella, que explica en sus Considerandos. Así, se identifican cuatro ámbitos a modificar. En concreto, la indemnización de los perjudicados en caso de insolvencia de la entidad aseguradora; los importes mínimos obligatorios de cobertura; los controles del seguro de los vehículos por parte de los Estados miembros; y el uso de las certificaciones de antecedentes sinistral de los titulares de pólizas por una nueva entidad aseguradora. Además, la Directiva determina la conveniencia de modificar los vehículos expedidos; los accidentes en que esté implicado un remolque arrastrado por un vehículo; las herramientas independientes de comparación de precios de seguros de vehículos automóviles; los organismos de información; y la información a los perjudicados. Finalmente, señala la norma, debe mejorarse la claridad de la Directiva 2009/103/CE, sustituyendo el término «víctima», que hasta entonces utilizaba como sinónimo de «perjudicado», por el término «perjudicado».

Por otra parte, la Directiva 2021/2118 sigue prestando atención, pese a lo ya debatido, al concepto de «vehículo» y al de «circulación de vehículos», a raíz de algunas resoluciones del TJUE, en las que se aclara que los vehículos automóviles están destinados normalmente a servir como medio de transporte, con independencia de las características del vehículo, y que la circulación comprende toda utilización de un vehículo que sea conforme con su función habitual de medio de transporte, con independencia del terreno en el que se utilice y de si está parado o en movimiento. Por lo tanto, no se aplicaría la Directiva si la función habitual del vehículo no es la de medio de transporte.

Finalmente, en lo que nos interesa, la Directiva del año 2021 insta a la Comisión Europea a supervisar y revisar la Directiva 2009/103/CE, a la luz de la evolución tecnológica, teniendo presente asimismo el mayor uso de vehículos autónomos y semiautónomos.

En resumen, de lo antedicho cabe extraer que el juego de la responsabilidad civil automovilística y su aseguramiento se asienta sobre varios elementos, en los que hemos de detenernos, siquiera brevemente, a los efectos de

²⁵ Vid. *infra* la exégesis que hace el TJUE del concepto de «vehículo a motor» o de «hecho de la circulación», entre otros.

concluir si el vigente régimen legal se adecúa o no a las particularidades que presentan los vehículos automatizados o si, por el contrario, se aconseja optar por uno nuevo y diferente. Estos elementos son el concepto de «vehículo a motor», el de «hecho de la circulación» y, por último, el de «conductor».

2.2. EL CONCEPTO DE «VEHÍCULO A MOTOR»

Para definir «vehículo a motor» hemos de acudir, en primera instancia, al concepto que contempla la Directiva 2009/103/CE. Esta norma, en contraposición al RSOA, acoge una expresión mucho más amplia que la de nuestra vigente legislación al contemplar, simplemente, el término «vehículo», y no el de «vehículo a motor». Con todo, el art. 1 de la Directiva, por su dicción, asimila uno y otro término al delimitar el primero como «todo vehículo automóvil destinado a circular por el suelo, accionado mediante una fuerza mecánica y que no utiliza una vía férrea, así como los remolques, incluso no enganchados».

No obstante lo señalado por la subrayada Directiva del año 2009, la 2021/2118 modifica este último extremo e incorpora algunos matices a tener en cuenta, por cuanto la definición de vehículo, a raíz de las nuevas formas de circulación, debe restringirse, basándose, según el legislador comunitario, en las características generales de dichos vehículos²⁶. A este respecto, la norma entiende como «vehículo»: «a) todo vehículo automóvil accionado exclusivamente mediante una fuerza mecánica que circula por el suelo y que no utiliza una vía férrea, con: i) una velocidad máxima de fabricación superior a 25 km/h, o ii) un peso neto máximo superior a 25 kg y una velocidad máxima de fabricación superior a 14 km/h; b) todo remolque destinado a ser utilizado con uno de los vehículos a que se refiere la letra a), tanto enganchado como no enganchado».

Además, sin perjuicio de lo dispuesto en las letras a) y b), excluye las sillas de ruedas que se destinen, en exclusiva, a ser utilizadas por personas con discapacidad física.

Por otro lado, el art. 3 insta a los Estados miembros a que adopten cuantas medidas resulten oportunas para que la responsabilidad civil surgida de la circulación de vehículos, que tengan su estacionamiento habitual en su te-

²⁶ En concreto, la Directiva 2021/2118 atiende, en particular, a la velocidad máxima de fabricación y el peso neto del vehículo, debiendo entrar dentro del ámbito del concepto tan solo los que estén accionados exclusivamente mediante una fuerza mecánica, y con independencia del número de ruedas que pudiera tener. De igual modo, no considera vehículo las sillas de ruedas destinadas a ser utilizadas por personas con discapacidad física, tal y como ahora explicitaremos en el cuerpo del presente.

ritorio, determinado por su matrícula o signo distintivo que los identifique, quede cubierta mediante un seguro. Ahora bien, la Directiva añade que no cabe exigir una cobertura de un SOA cuando el vehículo en cuestión haya sido dado de baja permanente o temporalmente, esté en fase de restauración o no se haya utilizado durante un largo período de tiempo por cualquier otro motivo, en virtud del apartado tercero del art. 5 Directiva 2009/103/CE, añadido por la 2021/2118.

En su posición de intérprete de la legislación comunitaria, el TJUE ha venido concretando los aspectos más significativos de lo que ha de comprenderse dentro de «vehículo» según la Directiva de referencia, y ha concluido de manera reiterada en su jurisprudencia que tendrá tal consideración el que sirva como medio de transporte, al margen del uso que se le esté dando por el particular, siempre que tenga su estacionamiento en un Estado miembro y no haya sido excluido expresamente de aseguramiento por razón de matriculación especial²⁷.

Centrándonos ahora en la normativa española, el concepto de «vehículo a motor» debe pasar irremediabilmente por el estudio del art. 1 RSOA, por cuanto el Reglamento, a los fines de la responsabilidad civil derivada de la circulación de vehículos a motor y de la obligación de aseguramiento, considera que coincidirá con todo vehículo idóneo para circular por la superficie terrestre e impulsado a motor, incluidos los ciclomotores, vehículos especiales, remolques y semirremolques, cuya puesta en circulación requiera autorización administrativa de acuerdo con lo dispuesto en la legislación sobre tráfico, circulación de vehículos a motor y seguridad vial. Y añade que, como excepción, quedan fuera de la obligación de aseguramiento los remolques, semirremolques y máquinas remolcadas especiales cuya masa máxima autorizada no exceda de setecientos cincuenta kilogramos, así como aquellos vehículos

²⁷ Muy ilustrativa es la STJUE, Sala Tercera, de 4 de septiembre de 2014, Asunto *Damijan Vnuk v. Zavarovalnica Triglav d.d.*, (C-162/13), (TJCE 2014,297), en la que se analiza la posible inclusión de un tractor dentro de la definición de «vehículo» del art. 1 Directiva 2009/103/CE y, en su caso, la obligación de asegurar necesariamente la responsabilidad civil en que pudiera incurrirse con su conducción.

En cuanto a la primera cuestión, el Alto Tribunal precisa que su encaje en el concepto no depende del uso que se haga o pueda hacerse del mismo, concluyendo que «Por lo tanto, el hecho de que un tractor, eventualmente dotado de remolque, pueda, en determinadas circunstancias, ser utilizado como maquinaria agrícola es irrelevante a efectos de la constatación de que tal vehículo responde al concepto de «vehículo»».

Por lo que respecta al deber de aseguramiento de la responsabilidad civil prevista en el art. 3 Directiva del año 2009, el TJUE advierte que, para que nazca, habrán de concurrir dos presupuestos. Uno, que «es necesario que ese vehículo tenga su estacionamiento habitual en el territorio de un Estado miembro». Y dos, que dicho Estado miembro no haya «excluido ese tipo de vehículo del ámbito de aplicación de la citada disposición», por haberle atribuido una matriculación especial, conforme al art. 4, letra b) de la Directiva.

que hayan sido dados de baja de forma temporal o definitiva del Registro de Vehículos de la Dirección General de Tráfico²⁸, en la línea de lo ya legislado por la Unión Europea.

En consecuencia y en atención a lo prevenido por el citado precepto, será «vehículo a motor» el que cumpla los siguientes presupuestos. En primer lugar, que sea apto para circular por la superficie terrestre; en segundo lugar, que esté propulsado por motor; y, en tercer lugar, que su puesta en circulación requiera de autorización administrativa, en virtud de lo reconocido por art. 59 del Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (Ley Tráfico, en lo sucesivo), -desarrollado por el art. 25 del Real Decreto 2822/1998, de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos, (RGV, en lo que sigue)-²⁹.

²⁸ Resulta interesante en este punto traer a colación el Proyecto de Ley por la que se modifica el texto refundido de la ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, (PL, desde ahora), habida cuenta de que incide en el concepto de «vehículo a motor» en un intento de armonizar la legislación comunitaria y nacional, y al mismo tiempo transponer la Directiva 2021/2118. En efecto, el PL pretende incorporar un nuevo artículo 1 bis al TRLRCSVM, en el que se determine cuándo estaremos, a los efectos de dicha ley y su normativa de desarrollo, ante un vehículo a motor, estableciendo que: «Se entiende por vehículo a motor: a) Todo vehículo automóvil accionado exclusivamente mediante una fuerza mecánica que circula por el suelo y que no utiliza una vía férrea, con: i. una velocidad máxima de fabricación superior a 25 km/h, o ii. un peso neto máximo superior a 25 kg y una velocidad máxima de fabricación superior a 14 km/h. b) Todo remolque destinado a ser utilizado con uno de los vehículos a que se refiere la letra a), tanto enganchado como no enganchado», excluyendo del ámbito objetivo tanto a los ferrocarriles, tranvías y vehículos que circulen por las vías que les sean propias, como a «las sillas de ruedas destinadas exclusivamente a ser utilizadas por personas con discapacidad física».

Parece claro que de la lectura del precepto transcrito se desprende que no estamos más que ante una simple traslación o transposición del contenido regulado en la Directiva 2021/2118 a la normativa interna española, sin que se añada cuestión alguna que desarrolle lo propugnado desde Europa.

²⁹ En efecto, el art. 59 Ley Tráfico dispone que «Con objeto de garantizar la aptitud de los conductores para manejar los vehículos y la idoneidad de estos para circular con el mínimo de riesgo posible, la circulación de vehículos a motor y de ciclomotores requerirá de la obtención de la correspondiente autorización administrativa previa», del permiso de circulación del vehículo y de la tarjeta de inspección técnica. En este sentido, el desarrollo del citado precepto se encomienda al RGV, en su art. 25, que establece que «Para poner en circulación vehículos de motor, así como remolques y semirremolques de masa máxima autorizada superior a 750 kilogramos, será preciso matricularlos y que lleven las placas de matrícula con los caracteres que se les asigne, del modo que se establece en el anexo XVIII. Esta obligación será exigida a los ciclomotores y ciclos de motor [...]». Y concluye, «Previamente a su matriculación, los vehículos citados en el apartado anterior deben estar dotados del correspondiente certificado oficial que acredite sus características técnicas esenciales y su aptitud para circular por las vías públicas, que se expedirá: a) Por los órganos competentes de la Administración o entidades delegadas, si se trata de vehículos que corresponden a tipos homologados incompletos, no homologados, matriculados anteriormente en otro país, vehículos usados procedentes de subastas oficiales realizadas en España o vehículos nuevos adquiridos directamente

Sin perjuicio de lo anterior, cabe subrayar que, a pesar de que tan solo contemos con una única definición de «vehículo autónomo» en el marco de la legislación española, ubicada en la Instrucción 15/V-113, y que ya hemos tenido ocasión de explicitar anteriormente, lo cierto es que no podemos acudir a ella por varios motivos. El primero, por su carácter reglamentario, en tanto que interpretadora de normas *stricto sensu*³⁰. El segundo, por su objeto, cual es, en exclusiva, la regulación de la concesión de autorizaciones especiales para la realización de pruebas y ensayos de investigación con vehículos automatizados y autónomos en vías abiertas al tráfico en territorio nacional³¹. Y, el tercero, porque a este tipo de vehículos, *a priori*, no les es de aplicación la normativa sobre tráfico y circulación vial, toda vez que la Instrucción podría condicionar la circulación en pruebas a que el automóvil en cuestión tuviera suscrito un seguro distinto al de responsabilidad civil automovilística *ordinario*³². A mayor abundamiento, llama la atención que la propia Directiva 2021/2118 excluya del ámbito de aplicación de su articulado «la utilización de vehículos en eventos y actividades automovilísticos, incluidas carreras y competiciones, así como entrenamientos, pruebas y demostraciones, en particular de velocidad, fiabilidad o habilidad, que estén autorizados en virtud de su Derecho nacional». Y ello guarda cierta lógica, por cuanto el riesgo de sufrir un accidente se eleva exponencialmente por razón de la peligrosidad intrínseca que lleva consigo este tipo de actividades³³. Ergo, siguiendo este razonamiento, dado

en otro país y que posean un certificado de conformidad CE. b) si se trata de vehículo nuevo que corresponde a tipo homologado según la legislación nacional u homologación CE».

³⁰ SANTAMARÍA PASTOS (2016, 258 y ss.).

³¹ ELIZALDE SALAZAR (2022, 37).

³² Sobre esta cuestión es interesante el análisis que efectúa ZORNOZA SOMOLINOS (2021, 81-84), a partir del cual estima que «el vehículo automatizado en pruebas necesita de un seguro de responsabilidad civil que ofrezca las mismas coberturas económicas que el SOA, pero sin ser un SOA».

Esta consecuencia, en efecto, se infiere del texto de la Instrucción al declarar que «El propietario del vehículo autónomo o cualquier persona que tenga interés en su aseguramiento estará obligado a suscribir y mantener en vigor un contrato de seguro que cubra hasta la cuantía de los límites del aseguramiento obligatorio de vehículos a motor, así como la responsabilidad civil derivada de los posibles daños causados en las personas o los bienes con motivo de la circulación durante la realización de las pruebas en vías abiertas al tráfico en general».

Y es que lo cierto y verdad es que del tenor literal de la norma no es descabellado pensar que el propietario del vehículo automatizado, en el contexto explicado, habrá de contar con dos seguros de daños distintos o, al menos, con uno que alcance a la cobertura obligatoria del SOA y con otro de carácter voluntario -o de daños propios-.

Sin embargo, también es cierto que cabe la posibilidad de que el legislador estuviera pensando, al tiempo de la redacción, en un único seguro, encuadrable dentro del SOA, aunque finalmente materializara su voluntad, debido al empleo de una técnica legislativa mejorable, no de la forma más idónea, en tanto que habría incurrido en una reiteración innecesaria o expresión pleonástica.

³³ La Directiva 2021/2118 aclara que «Estas actividades exentas deben tener lugar en una zona restringida y demarcada de tal manera que se garantice que el tráfico ordinario, el público y cualquier persona no relacionada con la actividad no puedan compartir efectiva o potencialmente el

el elevado riesgo de siniestro que se plantea al tiempo de realizar testeos de vehículos de estas características, motivado por el estado actual de la técnica, y la imposibilidad de regular esta materia por las Directivas de los años 2009 y 2021, análoga conclusión debe alcanzarse en cuanto a la necesidad de rehusar el concepto de vehículo autónomo que emplea la Instrucción 15/V-113.

En base a todo ello, a nuestro juicio, nada obsta para que el vehículo automatizado o semiautomatizado se incluya dentro de la definición legal de vehículo a motor, llamémosle convencional, que emplea el RSOA -e incluso el PL-, aunque, eso sí, siempre que estuviera dotado, como no podía ser de otro modo, de motor y se hubiera homologado el vehículo en su conjunto o el sistema que permite la automatización, o bien se hubiera obtenido una homologación especial y provisional para componentes técnicos que no resultaran compatibles con la vigente legislación, conforme a lo indicado líneas atrás³⁴.

2.3. EL CONCEPTO DE «HECHO DE LA CIRCULACIÓN»

Hasta el año 2021, a escala comunitaria, no disponíamos de una definición legal de lo que debía entenderse por «hecho de la circulación». Ello cambia diametralmente con la promulgación de la Directiva 2021/2118, que modifica la Directiva 2009/103/CE en este punto, e introduce en su art. 1 un nuevo apartado, rubricado como 1 bis, en el que se describe lo que la norma conceptualiza como «circulación de un vehículo». Así, establece que «toda utilización de un vehículo que sea conforme con la función del vehículo como medio de transporte en el momento del accidente, con independencia de las características de este, del terreno en el que se utilice el vehículo automóvil y de si está parado o en movimiento», será «circulación de un vehículo» a efectos de la Directiva.

Por su parte, el art. 2 RSOA reza que serán «hechos de la circulación» por lo que respecta a la responsabilidad civil en la circulación de vehículos a motor y de su cobertura por el SOA, «[...] los derivados del riesgo creado por la conducción de los vehículos a motor a que se refiere el artículo anterior, tanto por garajes y aparcamientos, como por vías o terrenos públicos y privados ap-

itinerario recorrido. Estas actividades suelen incluir las que se desarrollan en circuitos o itinerarios destinados al automovilismo y en las zonas que se encuentran en sus inmediaciones, como las zonas de seguridad, las zonas destinadas a las paradas técnicas y los garajes, en las que el riesgo de accidente es mucho mayor en comparación con las carreteras normales y a las que no deberían acceder personas no autorizadas».

³⁴ Es por ello que coincidimos plenamente con el planteamiento que efectúa ZORNOZA SOMOLINOS (2021, 123) al apuntar, tal y como nosotros hacemos, que «el vehículo automatizado encajaría en el concepto de vehículo a motor del R.SOA».

tos para la circulación, urbanos o interurbanos, así como por vías o terrenos que sin tener tal aptitud sean de uso común».

Este último precepto concreta, pues, que el hecho de la circulación está intrínsecamente ligado a la acción de conducir un vehículo a motor³⁵. Sin embargo, como hemos puesto de manifiesto, el vehículo automatizado o semiautomatizado, en sus niveles más avanzados, por sí mismo, prescinde de tal acción, toda vez que es el propio *software* incorporado al equipo el que hace las veces de conductor.

A esta circunstancia se le une la exégesis *lato sensu* que viene haciendo el TJUE de la meritada expresión, cosa que redundará aún más si cabe en que a la hora de interpretar el sentido de esta locución se ponga el acento no tanto en la acción de conducir, como en la de circular³⁶.

Efectivamente, *ad exemplum*, el Alto Tribunal europeo ha dado cabida dentro del concepto de «circulación de un vehículo» a daños ocasionados por un vehículo con el motor parado por entender que los mismos forman parte del riesgo circulatorio³⁷; y lo mismo ocurre con los daños producidos a un vehículo por el pasajero de otro adyacente al abrir su puerta, estando ambos automóviles estacionados³⁸.

³⁵ Ríos de tinta han corrido en torno a si la actividad generadora de riesgo es la circulación de un vehículo o, por el contrario, su conducción. Para REGLERO CAMPOS (2014, 1604 y ss.) la circulación de un vehículo lleva implícita su conducción. En cambio, para ZORNOZA SOMOLINOS (2021, 126) el riesgo lo crea la propia conducción, que es la que se objetiviza, y no la circulación, lo que se justifica en que la imputación de responsabilidad lo sea por el riesgo que aquella entraña, al margen del elemento culpabilístico que haya podido mediar por parte del conductor. Nosotros no podemos compartir esta corriente de pensamiento, colocándonos en la línea que viene marcando tanto el legislador europeo, cuanto el TJUE y el TS español, en el sentido que se dirá.

³⁶ BADILLO ARIAS (2016, 178-189).

³⁷ A estos fines resulta cuando menos llamativa la argumentación empleada por el TJUE, Sala Segunda, en su Sentencia de 20 de junio de 2019, Asunto *Línea Directa Aseguradora, S.A. v. Segurcaixa, Sociedad Anónima de Seguros y Reaseguros*, (C-100/18), (TJCE 2019,111) para resolver el supuesto de hecho del que conoció. La sentencia traía causa de una cuestión prejudicial planteada por el Tribunal Supremo español, cuyo sustrato jurídico radicaba en decidir si, pese a encontrarse estacionado el vehículo en un garaje privado, los daños que había originado en el inmueble en el que se encontraba ubicado más de 24 horas después de su puesta en marcha, a resultas de su incendio por un cortocircuito eléctrico del propio vehículo, debían ser cubiertos por la póliza del SOA o, por el contrario, por el seguro del hogar. Pues bien, el TJUE concluyó que el concepto de «circulación de vehículos» comprende «cualquier utilización de un vehículo que sea conforme con su función habitual», no limitándose a situaciones de circulación en sentido estricto. Y, por lo tanto, el estar inmovilizado el automóvil al tiempo del siniestro no puede excluir, por sí solo, la función de medio de transporte que tiene.

³⁸ Vid. STJUE, Sala Sexta, de 15 de noviembre de 2018, Asunto «*BTA Baltic Insurance Company AS v. «Baltijas Apdrošināšanas Nams» AS*», (C-648/17), (JUR 2018,304727).

En consecuencia, parece que el TJUE y el TS³⁹ han adoptado, en los últimos años, una interpretación extensiva y generosa de la «circulación de un vehículo» o del «hecho de la circulación», respectivamente. Ello supone, en la práctica y desde nuestro prisma, que la normativa sobre responsabilidad civil derivada de la circulación de vehículos a motor y su aseguramiento sea compatible, hoy día, con las nuevas formas de conducción, con independencia del carácter convencional o automatizado de dichos vehículos. A saber, los daños provocados por un vehículo que se utilice como medio de transporte con ocasión de la circulación en sentido estricto, o los acaecidos estando el mismo parado cuando medie la preceptiva relación causal entre el evento dañoso y su uso, han de gozar del carácter automovilístico, tanto en lo que se refiere a su reparación, como en lo que afecta a su cobertura por el seguro obligatorio de responsabilidad civil suscrito. Esto será así siempre que, por descontado, el vehículo esté provisto de motor y cuente con la correspondiente autorización administrativa de acuerdo con lo dispuesto en la legislación sobre tráfico, circulación de vehículos a motor y seguridad vial, como ya se declaraba *ut supra*.

2.4. EL CONCEPTO DE «CONDUCTOR»

La Ley Tráfico, en su Anexo I, al cual remite expresamente el art. 3 de su articulado, comienza por conceptualizar el elemento subjetivo de la conducción, a saber, la figura del «conductor», disponiendo que será toda «Persona que [...] maneja el mecanismo de dirección o va al mando de un vehículo, o a cuyo cargo está un animal o animales. En vehículos que circulen en función de aprendizaje de la conducción, tiene la consideración de conductor la persona que está a cargo de los mandos adicionales»⁴⁰.

³⁹ Sobre la inclusión como «hecho de la circulación» de siniestros ocurridos con el vehículo parado se viene pronunciando desde hace años la Sala de lo Civil del TS. Entre otras, pueden citarse las siguientes SSTs, misma Sala, núm. 1116/2008, de 2 de diciembre, (RJ 2009,417); núm. 816/2011, de 6 de febrero, (RJ 2012,4983); núm. 415/2015, de 1 de julio, (RJ 2015,2557); o núm. 556/2015, de 19 de octubre, (RJ 2015,4896).

⁴⁰ Esta definición se construye a partir de los elementos recogidos en el art. 1, en relación con el art. 8 de la Convención sobre la circulación vial, firmada en Viena el 8 de noviembre de 1968, que prescriben que «conductor» será «toda persona que conduzca un vehículo, automóvil o de otro tipo (comprendidos los ciclos), o que por una vía guíen cabeza de ganado, solas o en rebaño, o animales de tiro, carga o silla», la cual «deberá poseer las cualidades físicas y psíquicas necesarias y hallarse en estado físico y mental de conducir» y, al mismo tiempo, «poseer los conocimientos y la habilidad necesarios para la conducción del vehículo». En cualquier caso, el precepto aclara que el conductor tendrá que disponer en todo momento del dominio de su vehículo o de poder guiar sus animales; y en el art. 4 de la Convención sobre circulación por carretera y transporte por vehículos automotores, firmada en Ginebra el 19 de septiembre de 1949, que dispone que coincidirá con «toda persona que conduzca un vehículo (inclusive bicicletas) o guíe animales de tiro, carga, silla o rebaños por una carretera, o que tenga a su cargo el control efectivo de los mismos».

De su análisis se extrae que el conductor *clásico* es aquel que tiene el control mecánico del vehículo y quien guarda la llave para promover su conducción. Ahora bien, el encontrarse al mando de este último no solo admite una interpretación en un sentido físico, sino que también se refiere al propio control o supervisión de su manejo. Ejemplo de ello da que la segunda parte de la definición apunte al hecho de que en los vehículos de aprendizaje asumirá el rol de conductor el que esté a cargo de los mandos adicionales.

Es en este punto donde entran en juego los ADAS incorporados a ciertos vehículos con distintos niveles de automatización (entre 1 y 3 SAE) y su relación con la obligación del conductor de supervisar la marcha, habida cuenta de que con estas nuevas tecnologías que ayudan a la conducción, algunas de las tareas que, desde antaño, descansaban en quien se ponía a los mandos del volante, ahora permiten desplazarlo a un segundo plano en según qué situación o circunstancia. Es decir, que los ADAS facultan al conductor para desatender algunas de las tareas que, de ordinario, estaba obligado a ejecutar, a fin de poder circular con su automóvil. Sin embargo, que la decisión mecánica se atribuya al sistema instalado en el vehículo no es sinónimo de que el sujeto que en él viaja se vea exonerado de responsabilidad en todo caso. Muy al contrario, cuando interfiera de un modo significativo en la causación del siniestro podrá verse obligado a responder del daño irrogado al tercero, y ello incluso cuando inicialmente el *software* pudiera adolecer de algún defecto, tal y como se dirá de inmediato.

3. LA INCIDENCIA EN LA CONDUCCIÓN AUTOMATIZADA DE LA NUEVA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL, Y SUS EVIDENTES DISFUNCIONALIDADES

Hemos dejado sentado que la conducción automatizada, en este momento, ya empieza a plantear problemas y retos jurídicos que resulta necesario abordar a la mayor brevedad desde el plano legislativo. En este sentido, hemos de tomar en consideración dos aspectos de vital importancia. De un lado, que las normas actualmente vigentes en materia de responsabilidad no fueron diseñadas para dar solución a la amalgama de posibilidades que pueden sur-

Sea como fuere, si bien España forma parte de la Convención de Ginebra, huelga decir que el legislador español se basó para la redacción de la ley nacional en la firmada en Viena, cuyo contenido resulta más preciso que el de aquel texto legal.

gir con ocasión de la circulación de vehículos autónomos⁴¹. De otro lado, que el uso de la IA, *per se*, conlleva una latente potencialidad dañina⁴², lo que supone que el mismo deba ser regulado de tal forma que se minimicen los riesgos de causar daños a terceros y, de producirse, resulte lo más sencillo posible identificar a los agentes intervinientes⁴³, en aras de imputarles responsabilidad, en aplicación del aforismo latino *non laedere alterum*, que vertebra todo el Derecho de Daños.

A este respecto, tal y como pone de manifiesto ARROYO APARICIO⁴⁴, surgen tres posibles soluciones en cuanto a la reglamentación de la responsabilidad derivada de la utilización de vehículos autónomos. En primer lugar, mantener el régimen actual sin efectuar reformas de calado. En segundo lugar, modificar la Directiva 85/374/CEE, sobre responsabilidad por daños causados por productos defectuosos o, en su caso, la Directiva 2009/103/CE, relativa al seguro de responsabilidad civil que resulta de aplicación a la circulación de vehículos. O, finalmente, introducir una nueva regulación que establezca un marco normativo de seguro, sin determinación de culpabilidad -o *no-fault insurance*⁴⁵, para el caso de que se originen daños causados por vehículos autónomos.

Por esta última alternativa han apostado algunos autores⁴⁶, prestándole mayor apoyo que la atención que le ha merecido al legislador comunitario

⁴¹ En efecto, tal y como advirtió la Comisión de Transportes y Turismo del Parlamento Europeo en su Informe sobre la conducción autónoma en los transportes europeos de fecha 5 de diciembre de 2018, «las normas sobre responsabilidad [en particular, la Directiva 2009/103/CE y la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos, (Directiva 85/374/CEE, en lo que sigue)] no fueron diseñadas para dar respuesta a los retos que plantea el uso de vehículos autónomos [...] y cada vez hay más pruebas de que el actual marco reglamentario, especialmente con respecto a la responsabilidad, las pólizas de seguro, el registro y la protección de los datos personales, ya no será suficiente ni adecuado cuando haya que hacer frente a los nuevos riesgos derivados del aumento de la automatización, la conectividad y la complejidad de los vehículos».

⁴² TAPIA HERMIDA (2020, 85).

⁴³ Y es que, según la Resolución del Parlamento Europeo, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos (2018/2089(INI)), «es necesario poder determinar de manera inequívoca quién es el culpable en cada caso particular» ante una más que probable intervención de pluralidad de sujetos responsables del daño.

⁴⁴ ARROYO APARICIO (2022, 138-139).

⁴⁵ Con todo, esta tipología de seguro no concilia ni con el seguro de responsabilidad civil *ex art. 73 y ss. Ley 50/1980, de 8 de octubre, de Contrato de Seguro, (LCS, desde ahora)*, ni con el de accidentes *ex art. 100 y ss. LCS*, lo que obligaría a configurar una nueva tipología -incorporada en la LCS o en una ley especial- con lo que ello supondría, habida cuenta de que, entre otras cuestiones, habría que diseñar su naturaleza, la cuantificación del daño, la eventual acción de repetición o las causas de exoneración del asegurador.

⁴⁶ ARROYO APARICIO (2022, 139); y ELIZALDE SALAZAR (2022, 165 y ss.).

hasta la fecha. Ello obedece, sin duda, al hecho de que este último ha decidido apartarse, al menos por ahora, de la política legislativa marcada inicialmente por la Propuesta de Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA, a partir de la cual, en síntesis, se fijaba un régimen de responsabilidad objetiva en aquellos casos en los que los llamados «sistemas de IA de alto riesgo» hubieran intervenido en la causación de daños, haciéndole responsable de su reparación al operador (inicial y final) del citado sistema⁴⁷.

En efecto, en estos momentos, la estrategia planteada por la Unión Europea pasa por aprobar tres grandes bloques normativos que pongan a las personas en el centro de la transformación digital, procurando el respeto de los valores fundamentales europeos, cuales son, como señala ORTIZ FERNÁNDEZ⁴⁸, la transparencia, la explicabilidad, la equidad, la rendición de cuentas, la responsabilidad y la fiabilidad.

En primer lugar, destaca el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA, en adelante)⁴⁹; en segundo lugar, la Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Propuesta de Directiva sobre responsabilidad en materia de IA, en lo sucesivo); y, por último, la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (Propuesta de Directiva sobre responsabilidad en materia de productos defectuosos, desde ahora), que está llamada a sustituir la vigente Directiva 85/374/CEE del año 1985.

Por razones metodológicas y de espacio, abordaremos de inmediato la incidencia que adquirirá la Propuesta de Directiva sobre responsabilidad en materia de IA, y sus disfuncionalidades con respecto al contenido regulatorio por el que se opta en la Propuesta de Directiva sobre responsabilidad en materia de productos defectuosos, en relación con la conducción automatizada,

⁴⁷ El art. 4 de la Propuesta de Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA, establecía que «El operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA».

Un análisis exhaustivo y crítico del contenido de la antedicha Propuesta de Resolución puede verse en LÓPEZ MAS (2024, 59-102).

⁴⁸ ORTIZ FERNÁNDEZ (2024, 3).

⁴⁹ DOUE núm. 1689, de 12 de julio de 2024.

dejando para un estudio posterior el examen detallado de este último texto legal.

3.1. ÁMBITO DE APLICACIÓN Y CARACTERES

El presupuesto esencial que condiciona todas las disposiciones que la Propuesta de Directiva sobre responsabilidad en materia de IA regula es que la misma tan solo será de aplicación, una vez aprobada, a aquellas demandas de responsabilidad civil de carácter extracontractual que estén basadas en el dolo o la culpa (responsabilidad civil subjetiva, *in fine*) por los daños y perjuicios causados por un sistema de IA. Con lo cual de este extremo se infiere que, en tanto que no se desarrollen normas generales a nivel comunitario que permitan a los perjudicados motivar sus demandas por los daños sufridos a causa del manejo de un sistema de IA, el Derecho sustantivo interno de los diferentes Estados miembro gozará de plena actualidad al verse en la imperiosa necesidad de colmar un no reducido vacío legal⁵⁰.

Y ya en este instante se plantea la primera duda en torno a la supuesta compatibilidad entre la Propuesta de Directiva y el TRLRCSCVM en el marco de la responsabilidad civil derivada de la circulación de vehículos automatizados. En efecto, la primera norma limita su ámbito objetivo a aquellas demandas sustentadas en el dolo o la culpa. Sin embargo, el TRLRCSCVM asume, como se sabe, un criterio de imputación diferente, en función de si el evento dañoso recae sobre una persona -responsabilidad objetiva- o, por el contrario, incide sobre un bien material -responsabilidad subjetiva-. En esta situación, de seguir transitando el legislador europeo el mismo camino que ha marcado hasta ahora, su homónimo español entendemos tendrá que tomar una decisión de calado. De un lado, modificar la normativa nacional, en el sentido de fijar un único criterio de imputación con independencia del bien que resulte dañado (previsiblemente, uno objetivo o cuasi-objetivo, en atención al riesgo inherente a la puesta en circulación de estos elementos peligrosos). O, de otro lado, aplicar la Propuesta de Directiva tan solo a aquellas demandas cuya pretensión se centre en reclamar responsabilidad por daños a las cosas, manteniendo el régimen jurídico actual del TRLRCSCVM.

Otra anomalía que pudiera surgir a este respecto es la no fácil conjugación entre la Propuesta de Directiva sobre responsabilidad en materia de IA

⁵⁰ Es la propia Exposición de Motivos de la Propuesta de Directiva sobre responsabilidad en materia de IA la que reconoce que «se espera que, si la UE no actúa, los Estados miembros adapten sus normas nacionales de responsabilidad civil a los retos que plantea la IA». Y sentencia «Esto dará lugar a una mayor fragmentación y a un aumento de los costes para las empresas que operan en la UE».

y la Propuesta de Directiva sobre responsabilidad en materia de productos defectuosos⁵¹. En este sentido, otro tanto de lo que se advertía con anterioridad ocurre si atendemos a la clase de responsabilidad que incorporan una y otra (subjettiva en la Propuesta de Directiva sobre responsabilidad en materia de IA, y objetiva en la Propuesta de Directiva sobre responsabilidad en materia de productos defectuosos). Y ello pese a que, en esta primera fase, como se dirá con mayor detalle *infra*, la Propuesta de Directiva sobre responsabilidad en materia de IA persigue limitar su rango de actuación a aspectos de índole probatoria al aligerar su carga por medio del uso de la exhibición de material probatorio y de presunciones refutables⁵², que no *iuris et de iure*⁵³, gracias a una fórmula de armonización mínima⁵⁴. Por el contrario, la relativa a productos defectuosos tiene un enfoque mucho más ambicioso, promoviendo adaptar, desde un punto de vista sustantivo, la Directiva 85/374/CEE a los productos con *softwares* de IA que adolezcan de defectuosidad, sin perjuicio de que también contenga reglas específicas para facilitar la prueba del meritado defecto, así como de la relación de causalidad. Asimismo, este cuerpo legal parte de una armonización plena por medio del diseño de una Directiva de máximos, vinculante para todos los Estados de la UE.

Precisamente esa es la razón que podría llevarnos a entender erróneamente que la Propuesta de Directiva sobre responsabilidad en materia de IA no va a interferir en la aplicación de la Propuesta de Directiva sobre responsabilidad en materia de productos defectuosos. No obstante, aunque aquella

⁵¹ Sobre la posible aplicación de la normativa en materia de productos defectuosos en nuestro ámbito de estudio se pronuncia ÁLVAREZ OLALLA (2019, 145-170).

⁵² Así y todo, tampoco se pretende con la Propuesta de Directiva sobre responsabilidad en materia de IA la armonización de las legislaciones nacionales ni en lo que se refiere al grado de certeza necesario para que exista fuerza probatoria, ni al sujeto sobre el cual pesará el *onus probandi*.

⁵³ La Exposición de Motivos de la Propuesta de Directiva sobre responsabilidad en materia de IA aboga por un avance paulatino, integrado por dos fases. «En la primera fase, los objetivos se alcanzan con un enfoque mínimamente invasivo; la segunda fase consiste en reevaluar la necesidad de medidas más estrictas o amplias. La primera fase se limita a las medidas relativas a la carga de la prueba para hacer frente a los problemas propios de la IA detectados», dejando la segunda velocidad para reevaluar otras medidas más estrictas o invasivas, que aconsejarían pasar por la exigencia de suscripción de seguros obligatorios y fórmulas de responsabilidad objetiva, como reconoce MARCHENA GÓMEZ, M. (2024, 287).

⁵⁴ O, dicho de otro modo, como expone RODRÍGUEZ DE LAS HERAS BALLELL (2023, 5), la Directiva sobre responsabilidad por productos defectuosos desempeña un papel clave y al ampliar su ámbito de actuación para incluir los bienes que utilizan inteligencia artificial se refuerza, amplía y aprovecha el potencial de armonización de la Directiva, que incluye una cláusula expresa de armonización plena.

Por ende, se deja a los Estados miembro libertad para legislar de manera más favorable para los demandantes, con el límite de, como no podía ser de otro modo, guardar respeto al resto de la normativa emanada de la Unión.

adopte un ámbito objetivo mucho más amplio⁵⁵, no es menos cierto que la compatibilidad entre ambas normativas no está en absoluto garantizada por los motivos anteriormente indicados.

En nuestro caso, creemos que tanto las futuras Directivas sobre responsabilidad en materia de IA y de productos defectuosos, como la normativa patria, en especial, el TRLRCSVM adquirirán un papel importante en la concreción del régimen de responsabilidad civil al que se verá sujeto el operador de un vehículo automatizado, en la medida en que no contemos con un cuerpo legal definitivo que establezca normas sustantivas que definan su régimen jurídico.

3.2. DEBER DE EXHIBICIÓN DE PRUEBAS Y PRESUNCIÓN *IURIS TANTUM* EN CASO DE INCUMPLIMIENTO

Cuando estamos ante sistemas de IA de alto riesgo, cualidad esta que habrá de verificarse acudiendo al concepto que configura el Reglamento de IA⁵⁶, los perjudicados por el daño podrán exigir que el órgano jurisdiccional

⁵⁵ Lo pone de manifiesto MARTÍN CASALS (2023, 71).

⁵⁶ Efectivamente, el art. 2 Propuesta de Directiva sobre responsabilidad en materia de IA reconoce como «sistema de IA de alto riesgo» aquel sistema que tenga dicha consideración de acuerdo con lo dispuesto en el art. 6 Reglamento de IA, el cual a su vez exige a tal efecto que el *software*, en general, reúna las dos condiciones siguientes: «a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I».

En el supuesto de los vehículos dotados de autonomía se da cumplida cuenta de la concurrencia de ambos presupuestos. En primer lugar, el dispositivo que a ellos se incorpora tiene la consideración de componente de seguridad del producto (esto es, el vehículo) que entra dentro del ámbito objetivo de los actos legislativos de armonización de la UE, en concreto, de un lado, del Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos; y, de otro lado, del mencionado anteriormente Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública. Y, en segundo lugar, el producto habrá de ser sometido, dada su latente peligrosidad, a una evaluación de conformidad con carácter previo a su introducción en el mercado.

Por ello, a nuestro entender, no cabe duda alguna de que los vehículos autónomos habrán de ser clasificados como sistemas de alto riesgo a todos los efectos y sus comercializadores someterse al especialmente riguroso régimen obligacional al que los sujeta el Reglamento de IA.

competente ordene a quien ostente información y pruebas relevantes necesarias para plantear de manera adecuada la correspondiente demanda -en particular, proveedores, fabricantes, representantes autorizados, importadores o distribuidores- que se las faciliten. Para ello, será preceptivo que, con carácter previo, el potencial demandante haya expuesto aquellos hechos o indicios de los que tenga conocimiento y sirvan para sustentar la viabilidad de su pretensión, pero, también, que haya desplegado esfuerzos razonables a fin de obtener las pruebas pertinentes de quien las tuviera a su alcance.

Con todo, la Propuesta de Directiva limita esta prerrogativa «a lo necesario y proporcionado para sustentar una demanda potencial o una demanda por daños y perjuicios», debiendo salvaguardarse los intereses legítimos relativos a la protección de secretos comerciales y de información confidencial, como la relacionada con la seguridad pública o nacional (art. 3.4 Propuesta de Directiva sobre responsabilidad en materia de IA).

Así, se trata de garantizar un justo equilibrio entre el derecho del dañado a ejercitar su derecho a obtener una tutela judicial efectiva, que, de lo contrario, podría verse comprometido, y el de las empresas a innovar en el sector de la IA. Y es que hemos de recordar que cuando de sistemas de IA de alto riesgo se trata, el Reglamento de IA exige que se cumplan una serie de requisitos de gestión de riesgos y datos, documentación, información o registro, y puede resultar particularmente compleja la obtención de estos datos, toda vez que el perjudicado no tiene *a priori* derecho a acceder a ellos⁵⁷.

Por lo demás, de incumplirse la orden del órgano jurisdiccional por parte del demandado, cabrá presumir probados aquellos hechos sobre los cuales se solicitaba la información y/o pruebas. Sin embargo, el demandado podrá destruir a través de cualquier medio admitido en Derecho la reseñada presunción, pues admite prueba en contrario.

3.3. PRESUNCIÓN *IURIS TANTUM* DE LA RELACIÓN DE CAUSALIDAD EN CASO DE CULPA

La cadena de personas intervinientes en el proceso de diseño, desarrollo y actualización del *software*, que suele ser considerable, es un factor que ha de

⁵⁷ Señala la Propuesta de Directiva sobre responsabilidad en materia de IA en su Considerando 16 que, por otra parte, establecer normas sobre la exhibición de los medios de prueba pertinentes puede suponer un incentivo para el sector empresarial, en el bien entendido de que se vea compelido gracias a esta reglamentación a cumplir con los requisitos que el Reglamento de IA impone.

Esta afirmación no sorprende, por cuanto el sector corporativo se ha venido mostrando reticente y contrario desde las primeras propuestas legislativas emanadas de la Unión Europea en materia de IA a la aprobación de una reglamentación estricta que pudiera desincentivar la inversión en esta clase de tecnología. *Ad exemplum*, MORENO IZQUIERDO; y PEDREÑO MUÑOZ (2020).

tenerse en cuenta al objeto de no solo identificar a la persona potencialmente responsable del daño⁵⁸, sino también de reconstruir el *iter* fáctico o, si se quiere, de conocer qué es lo que pudo desencadenar el hecho dañoso. Estamos, pues, ante la ardua tarea de acreditar la relación de causalidad entre la culpa y el daño sufrido, a resultas del uso de un vehículo automatizado dotado de IA.

Siguiendo esta premisa, el art. 4 Propuesta de Directiva sobre responsabilidad en materia de IA construye una presunción *iuris tantum* del nexo de causalidad a favor del perjudicado, eximiéndole de probar aquello que efectivamente pudo provocar el nacimiento del evento lesivo. Pero para que ello aplique la norma exige el cumplimiento de varios presupuestos.

En primer lugar, la acreditación por el demandante de la culpa del demandado, bien directamente, bien a través del mecanismo que examinábamos *ut supra*. Ahora bien, esa falta de diligencia necesariamente ha de coincidir con una infracción de un deber de cuidado que esté destinado directamente a proteger frente a los daños que se hayan producido. En consecuencia, no cabe predicar la culpa de todo incumplimiento, sino solamente de la contravención de la obligación que persiga evitar el perjuicio⁵⁹, conforme al concepto que recoge la Propuesta de Directiva. Así las cosas, dado que el Reglamento de IA armoniza las obligaciones específicas que han de asumir los proveedores o personas sujetas a esas mismas obligaciones, la culpa a considerar será la que dimane de su vulneración. De hecho, el apartado segundo del art. 4 Propuesta de Directiva sobre responsabilidad en materia de IA aclara que este requisito (la concurrencia de la culpa), cuando la demanda se dirija frente a proveedores, o personas sujetas a análogas obligaciones, «solo se cumplirá cuando el demandante haya demostrado que el proveedor o, en su caso, la persona sujeta a las obligaciones del proveedor» ha incumplido cualquiera de los condicionantes siguientes: (1) que se incumplan los criterios de calidad expuestos en el Reglamento de IA cuando estemos ante sistemas que utilicen técnicas que impliquen el entrenamiento de modelos con datos; (2) que el sistema se haya desarrollado sin cumplir los requisitos de transparencia exigidos por el Reglamento de IA; (3) que el sistema no permita una vigilancia efectiva por personas físicas durante el período en que esté en uso; y (4) que no se adopten de forma inmediata las medidas correctoras necesarias para poner el sistema de IA en conformidad con las obligaciones establecidas en el Reglamento de IA o para retirar del mercado o recuperar el sistema.

⁵⁸ NÚÑEZ ZORRILLA (2023, 830).

⁵⁹ Piénsese, por ejemplo, en un accidente de circulación que trae causa de la omisión de incluir expresamente en las instrucciones proporcionadas por parte del fabricante del sistema de IA incorporado a un vehículo el deber de actualización del *software*, en aras de una correcta y segura conducción en modo automático.

En segundo lugar, que la culpa del demandado haya influido, en atención a las circunstancias del caso y tomando un criterio de razonabilidad, en la respuesta que hubiera tenido el sistema de IA. Del tenor del precepto parece que el legislador para conectar la culpa «con los resultados producidos por el sistema de IA o [con] la no producción de resultados por parte del sistema de IA» ha escogido un criterio de imputación objetiva, que parte de la consecuencia probable. Esto es, a nuestro juicio, toma un modelo probabilístico que impide dar por cierta la relación de causalidad (*rectius* presumirla) a no ser que el hecho dañoso se hubiera producido de manera verosímil precisamente por la intervención del elemento subjetivo, o culpa. Este criterio no puede ser otro que el conocido como teoría de la adecuación⁶⁰.

Y, por último, la prueba por la actora de que «la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA causó los daños».

Desde nuestro prisma, el estándar de razonabilidad empleado por la Propuesta de Directiva para la acreditación del grado de influencia que pudo tener la culpa en la respuesta del *software* adquiere su razón de ser en este último requisito, habida cuenta de que es aquí donde el perjudicado se va a ver obligado a enfrentarse a verdaderos retos para establecer una relación causa-efecto entre el déficit del sistema de IA y el daño irrogado. A nuestro parecer, carece de sentido pergeñar mecanismos artificiosos con tal de salvaguardar la vigencia de una más que cuestionable filosofía que engendra la Propuesta de Directiva, que no es otra que la de exigir la concurrencia de la culpa. Quizás, en tanto que nos encontramos ante actividades ciertamente peligrosas, donde no siempre es sencillo conocer a ciencia cierta lo que pudo generar el siniestro, ni a quién en última instancia ha de atribuírsele la responsabilidad por ello, nos inclinamos por pensar que la opción más sensata fue la que adoptó inicialmente la Propuesta de Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA, la cual prescindió directamente del elemento subjetivo en supuestos de sistemas de IA de alto riesgo.

Con independencia de lo anterior, en supuestos en los que los daños hayan sido causados por usuarios del sistema de IA de alto riesgo, también cabrá presumir la relación de causalidad si estos no han utilizado o supervisado el sistema de IA de conformidad con las instrucciones de uso, o bien han expuesto al sistema de IA a datos de entrada bajo su control que no eran pertinentes

⁶⁰ En otro trabajo tuvimos la oportunidad de analizar con detalle la relación de causalidad desde el punto de vista físico y jurídico en nuestro ordenamiento jurídico, al cual nos remitimos por economía. LÓPEZ MAS (2021, 214 y ss.).

según la normativa aplicable. En cambio, cuando el usuario utilice el sistema de manera no profesional no regirá la meritada presunción⁶¹, a salvo que haya interferido sustancialmente en el funcionamiento del sistema de IA⁶², o tuviese la obligación y, además, pudiera determinar las condiciones de funcionamiento del mismo y no lo haya hecho. En otras palabras, se sanciona al usuario particular del *software* presumiendo el nexo causal cuando, encontrándose en una mejor posición que la actora a fin de determinar lo sucedido en el caso concreto, no proporcione una explicación razonable al respecto.

Con todo, el demandado siempre tendrá en su mano la facultad de desvirtuar la presunción a la que venimos refiriéndonos, pues se configura con el carácter de *iuris tantum*.

4. BIBLIOGRAFÍA

- ÁLVAREZ OLALLA, P., (2019). Responsabilidad civil en la circulación de vehículos autónomos. En A. Muñoz Villarreal (Coord.) y E. Monterroso Casado (Dir.). *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Valencia: Tirant lo Blanch (pp. 145-170).
- ARROYO APARICIO, A. (2022). Vehículos autónomos, responsabilidad y seguro. Avances legislativos y perspectivas. *Revista de Derecho del Sistema Financiero*, núm. 3, 127-150.
- BADILLO ARIAS, J. A. (2016), *La responsabilidad civil automovilística: el hecho de la circulación*. Cizur Menor: Aranzadi.
- BELÓN LAURÍN, J. A. (2022). Los vehículos autónomos y su seguro ¿hacia dónde vamos? *RRCCS*, núm. 4, 7-18.
- ELIZALDE SALAZAR, I. (2022). *Vehículos autónomos. Responsabilidad civil y seguro*. Cizur Menor: Aranzadi.
- LIN, P. (2016). Why Ethics Matters for Autonomous Cars. En M. Maurer; J. C. Gerdes; B. Lenz; H. Winner (Ed.). Heidelberg: Springer Berlin, (pp. 69-85).
- LIN, P.; JENKINS, R.; ABNEY, K. (2017). *Robot Ethics 2.0: From Autonomous Cars to Artificial intelligence*. New York: Oxford University Press.
- LÓPEZ MAS, P. J. (2021). *El lucro cesante. Configuración actual y criterios para su determinación judicial*. Madrid: Dykinson.

⁶¹ El fin que busca la norma es palmario: lograr un equilibrio entre los intereses de los perjudicados y de los usuarios que actúan como particulares. En este sentido, *vid.* NÚÑEZ ZORRILLA, C. (2023), p. 831.

⁶² En nuestro supuesto, podría referirse tal contribución a un mal uso, o a una manipulación, del sistema de IA incorporado al vehículo por parte del usuario, que fuera causa determinante del daño.

- LÓPEZ MAS, P.J. (2024). La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento. *RCDI*, Año núm. 100, núm. 801, 59-102.
- MARCHENA GÓMEZ, M. (2024). Inteligencia artificial y responsabilidad civil. En M. J. Herrador Guardia (Dir.). *Daño y resarcimiento*, Madrid: Sepín, (pp. 265-290).
- MARTÍN CASALS, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, núm. 3, 55-100.
- MORENO IZQUIERDO, L.; y PEDREÑO MUÑOZ, A. (2020). *Europa frente a EE.UU. y China. Prevenir el declive en la era de la inteligencia artificial (Retos en la era de la inteligencia artificial)*, España: KDP.
- NÚÑEZ ZORRILLA, C. (2023). La nueva directiva europea sobre responsabilidad civil por productos defectuosos y su aplicación a los vehículos totalmente automatizados o autónomos. *RCDI*, Año núm. 99, núm. 796, 801-851.
- ORTIZ FERNÁNDEZ, M. (2024). La «adaptación» del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad. *IDP*, núm. 40, 1-12.
- REGLERO CAMPOS, L. F. (2014). Responsabilidad civil y seguro en la circulación de vehículos de motor. En L. F. Reglero Campos y J. M. Busto Lago (Coord.). *Tratado de Responsabilidad Civil*, 2ª ed., T. I, Cizur Menor: Aranzadi, (pp. 1557-1892).
- RODRÍGUEZ DE LAS HERAS BALLELL, T. (2023). La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial. *La Ley mercantil*, núm. 103 (junio), 1-14.
- SANTAMARÍA PASTOS, J. A. (2016). *Principios de derecho administrativo general*, 4ª ed. Madrid: Iustel.
- SOTO NIETO, F. (1989). *Responsabilidad civil derivada del accidente automovilístico: (seguro de suscripción obligatorio)*. Madrid: La Ley.
- TAPIA HERMIDA, A. J. (2020). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. *RRCS*, núm. 76, 79-104.
- TORROBA DÍAZ, J. (2019). La responsabilidad civil derivada de la circulación de vehículos autónomos. *RRCCS*, núm. 1, 6-26.
- ZORNOZA SOMOLINOS, A. (2021). *Vehículos automatizados y seguro obligatorio de automóviles. Estudio de Derecho comparado*. Madrid: Dykinson.

Inteligencia artificial en la prestación de servicios de salud: funcionalidades, riesgos y responsabilidad civil⁶³

RAQUEL LUQUIN BERGARECHE

*Profesora Titular de Derecho civil.
Universidad Pública de Navarra*

Sumario: I. INTRODUCCION. ROBOTS Y APLICACIONES DE INTELIGENCIA ARTIFICIAL COMO INSTRUMENTOS AUXILIARES EN LA PRESTACION DE SERVICIOS MEDICOS. II. LA PREVENCIÓN DE LOS RIESGOS DE LA IA EN SALUD A LA LUZ DEL REGLAMENTO UE 2024/1689 DE 13 DE JUNIO DE 2024 (RIA). 2.1. Primer marco regulatorio europeo de la inteligencia artificial. 2.2. Inteligencia artificial y Salud: la definición de la IA de alto riesgo. 2.3. Obligaciones de proveedores y responsables del despliegue: información y supervisión. 2.4. Aplicaciones de IA en salud para uso particular o doméstico. 2.5. El RIA como ecosistema normativo de prevención: la remisión a otros sistemas regulatorios en el ámbito de los daños causados por sistemas de IA en salud. 2.6. Formación y capacitación del profesional de la salud en inteligencia artificial. III. DAÑOS CAUSADOS EN LA INTERVENCIÓN MÉDICA CON AUXILIO DE IA: REDEFINICIÓN DE LA “LEX ARTIS” Y FUNDAMENTOS DE LA RESPONSABILIDAD. 3.1. Cuando el médico se prevale en su actuación de un sistema de IA y causa daños: presupuestos de la obligación de responder. 3.2. Caracteres de los sistemas IA en salud: en particular, la influencia del grado de autonomía del robot o sistema auxiliar de IA en la responsabilidad por daños. 3.3. La relación de causalidad: causalidad física y su prueba. 3.4. La causalidad jurídica: el juicio de imputación. 3.5. Agentes implicados en la prestación de servicios médicos auxilio de

⁶³ Este trabajo se ha realizado en el marco del Proyecto de Investigación “Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos” CODISEMED (TED2021-129472B-00/MICINN “Next Generation EU”/PRTR).

IA. A. *El productor: fabricante o diseñador de la IA.* B. *El “responsable del despliegue” usuario profesional.* C. *El usuario no profesional de un sistema de IA.* **3.6. Causas de exoneración.** 4. ALGUNAS REFLEXIONES SOBRE EL RÉGIMEN (NO ARMONIZADO Y “DE MÍNIMOS”) DE LA PROPUESTA DE DIRECTIVA RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL A LA IA (PDRCIA) 5. REFERENCIAS BIBLIOGRÁFICAS.

1. INTRODUCCION. ROBOTS Y APLICACIONES DE INTELIGENCIA ARTIFICIAL COMO INSTRUMENTOS AUXILIARES EN LA PRESTACION DE SERVICIOS MEDICOS

La irrupción del nuevo paradigma de Salud Digital y la rápida implementación en este ámbito de tecnologías avanzadas y de inteligencia artificial plantea en el ámbito jurídico numerosas cuestiones: entre otras, las relativas a la salvaguarda de derechos de la personalidad como la intimidad y la protección de los datos personales de salud, especialmente sensibles, la redefinición del conjunto de derechos y deberes de las partes de la relación médico-paciente, el protagonismo activo del paciente y la responsabilidad civil por daños.

En este capítulo intentaremos dar respuesta al interrogante acerca de si debe responder el médico digital, y en caso afirmativo, en qué casos y bajo qué fundamentos, de los daños causados en el ejercicio de sus funciones por incumplimiento de los deberes que configuran su “lex artis” cuando en su actuación profesional (diagnóstica o pronóstica, terapéutica, quirúrgica o rehabilitadora) se auxilia por robots o sistemas de IA. Es decir: cuando utiliza cualquier “sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la adopción de medidas, con cierto grado de autonomía, para lograr objetivos específicos”.

Utilizar o valerse como elemento auxiliar de la inteligencia artificial como un apoyo a toma de decisiones del médico, además de redefinir la relación médico-paciente, incide en la “lex artis ad hoc” del profesional y, consiguientemente, en el modo en que éste resulta en su caso obligado a responder jurídicamente, en su caso, a responder jurídicamente de la indemnización del daño causado por su actuar culposo o negligente (por supuesto, doloso, conforme a las normas generales). Como dice el Tribunal Supremo en Sentencia 23 de mayo de 2006 “[...] *criterio valorativo para calibrar la diligencia exigible en todo acto o tratamiento médico, en cuanto comporta no sólo el cumplimiento formal y*

protocolar de las técnicas previstas con arreglo a la ciencia médica adecuadas a una buena praxis, sino la aplicación de tales técnicas con el cuidado y precisión exigible de acuerdo con las circunstancias y los riesgos inherentes a cada intervención según su naturaleza y circunstancias". En pronunciamiento posterior, en la STS de 16 de enero de 2008 (RJ/2008/4) afirma que *"el médico asume una obligación de medios y como tal se compromete no solo a cumplimentar las técnicas previstas para la patología en cuestión, con arreglo a la ciencia médica adecuada a una buena praxis, sino a aplicar tales técnicas con el cuidado y precisión exigible de acuerdo con las circunstancias y los riesgos inherentes a cada intervención (...)"* (en el mismo sentido, STS de 18 diciembre de 2006).

Es sabido que, para ponderar o calibrar la responsabilidad que deriva del incumplimiento de la *"lex artis ad hoc"*, debe atenderse el médico a las reglas de la experiencia, el estado de la ciencia y las circunstancias de tiempo y lugar⁶⁴. En un reciente pronunciamiento (STS 680/2023, de 8 de mayo de 2023) el Alto Tribunal enumera las implicaciones que comprende cuando afirma que *"[...] la lex artis abarca la utilización de los medios y técnicas necesarias, que el estado actual del conocimiento de la medicina, posibilita para el diagnóstico de las enfermedades, de manera proporcional al cuadro clínico que presenta el enfermo; seguir las prevenciones aceptadas por la comunidad científica para el tratamiento de la patología padecida; la práctica diligente de las técnicas empleadas en el proceso curativo, comprendiendo las quirúrgicas; la prestación de la información precisa, con antelación temporal suficiente, de manera comprensible, sobre el diagnóstico, pronóstico, tratamiento, riesgos típicos y prevenciones a seguir en el proceso de curación de la enfermedad; abstenerse de actuar en contra o al margen del consentimiento informado del paciente, que habrá de obtenerse, con mayor rigor, en el caso de la medicina voluntaria o satisfactiva; cumplimentar los deberes de la documentación clínica, sin incurrir en omisiones relevantes e injustificadas; y actuar siempre, de forma diligente, mediante el control de las incidencias del curso de la patología, sin incurrir en descuidos inasumibles, hasta el alta del paciente, con las indicaciones correspondientes de seguimiento, si fueran procedentes (prevenciones pautadas y revisiones periódicas en su caso)"*.

La irrupción de esta tecnología y su aplicación actual en el diagnóstico y tratamiento de enfermedades permite afirmar, a falta aún de resoluciones jurisprudenciales sobre los sistemas de inteligencia artificial en salud, que estas *"técnicas"* a las que se refieren los tribunales incluyen la medicina auxiliada por sistemas de inteligencia artificial.

⁶⁴ SSTS 8-5-1991, (RJ 1991/3618, 9-12-1999 (RJ 1999/8173), 14.5.2001 (RJ 2001/6204).

Además de las normas jurídicas que debe tener en cuenta el médico en el ejercicio de su profesión cuya inobservancia o defectuoso cumplimiento puede ser causa de infracción de la “lex artis”, SOLE FELIU se refiere a los principios, protocolos sanitarios, directrices o guías de práctica clínica⁶⁵: tanto el legislador español como la jurisprudencia relativa a la responsabilidad civil de los profesionales sanitarios utilizan las expresiones *protocolos* y *guías* de forma indistinta⁶⁶. La jurisprudencia española alude frecuentemente a la necesidad de que los tribunales acudan a los protocolos, directrices, recomendaciones, guías de práctica clínica, etc., como “elementos de apoyo” a la hora de configurar el contenido del deber de diligencia del profesional sanitario⁶⁷ (entre otras, citadas por el autor: SSTs, 3^a, 21.2.2008 [RJ 2008\1247]; 25.6.2010 [RJ 2010\5886]; 1^a, 29.1.2010 [RJ 2010\418]; SSAP Guipúzcoa 15.1.2007 [AC 2007\766]; SAP Asturias 7.7.2021 [JUR 2021\303748])⁶⁸. Valor también reconocido por nuestra doctrina, que los considera “fuente indirecta con un valor clave, incorporada a nuestro ordenamiento jurídico (...), en orden a valorar la conducta del médico y del profesional sanitario en su actuación médico-hospitalaria”⁶⁹, en plena coincidencia, en este punto, con la doctrina comparada. En lo que se refiere a su valor jurídico, el art. 4.7.b) de la Ley 44/2003, de 23 de noviembre, de ordenación de las profesiones sanitarias declara que los protocolos “deberán ser utilizados *de forma orientativa*, como guía de decisión, para todos los profesionales de un equipo”. Así lo confirman los tribunales,

⁶⁵ SOLE FELIU, J. “Responsabilidad civil y telemedicina: el valor de las guías de práctica clínica y protocolos en la determinación del estándar de diligencia”, LUQUIN BERGARECHE, R. (Dir.) *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.

⁶⁶ En este sentido, SOLE FELIU, J. “Estándar de diligencia médica y valor de los protocolos y guías de práctica clínica en la responsabilidad civil de los profesionales sanitarios”, *Revista de Derecho Civil*, vol. IX, núm. 3 (julio-septiembre, 2022), 1-52, pp. 26-29.

⁶⁷ Vid. STS 5.12.2006 [RJ 2007\232] en la que el tribunal afirma que las reglas deontológicas carentes de fuerza coactiva “no significa que no sirvan para configurar principios jurídicos que descansan sobre determinados valores o concepciones éticas, que inciden en la praxis médica y sirven para definir el contenido de los deberes profesionales que deben cumplirse en la actividad sanitaria. De este modo, las normas de deontología profesional y los estatutos de los colegios profesionales sirven de guía, y de modo decisivo, no solo para fijar los protocolos de actuación médica, sino especialmente para valorar la conducta del facultativo y su adecuación a la diligencia de un buen profesional, a los dictados, en suma, de la *lex artis ad hoc*” (FD 3).

⁶⁸ En la SAP Pontevedra (Sección 6^a) 10.10.2017 [AC 2017\137], la Audiencia Provincial tomó los protocolos como criterio de referencia a la hora de decidir, entre los diversos informes periciales -contradictorios- aportados al juicio a cuál de ellos daba mayor credibilidad, al entender que los protocolos aprobados por la Sociedad Española de Ginecología y Obstetricia, “*de referencia para ginecólogos y obstetras, ha de servirnos de guía para valorar los informes y dictámenes emitidos en este proceso*”.

⁶⁹ FERNÁNDEZ COSTALES, J., “Estado actual de la casuística de la responsabilidad sanitaria”, en MORENO MARTÍNEZ, J. A. (Coord.), *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007, p. 267. En la misma línea, señala GALÁN CORTÉS, *Responsabilidad civil médica*, 6^a, cit., pp. 278-279, que, aunque este tipo de normas “carecen de juridicidad, pueden ser acogidas como reglas por el juez para configurar el deber objetivo de cuidado en el caso concreto que se le plantea”.

expresiones como las contenidas en la SAP Cádiz 17.9.2002 [AC 2002\1929], según la cual “*los protocolos ...aconsejan, y no prescriben*”; o la SAP Guipúzcoa 15.1.2007 [AC 2007\766], la cual, citando la sentencia de primera instancia, declara que “*los protocolos médicos...operan como pautas, directrices o recomendaciones*”. O la SAP Madrid 1.3.2005 [AC 2005\521] cuando dice que “*no es necesaria ni preceptiva la existencia de protocolos médicos de actuación concretos, ni tiene que actuar el facultativo de conformidad con lo que en cada uno de ellos [se] señale*”.

En cualquier caso, la realidad normativa (y, consiguientemente, la jurisprudencial) van muy por detrás de la tecnológica: la IA lleva tiempo implementándose en servicios médicos, hallándose ya plenamente integrada en las “técnicas” utilizadas conforme al “estado de la ciencia” al que se refieren estas resoluciones. Por lo que deben tomarse en consideración por centros y profesionales sanitarios, públicos y privados, no con una fe o “confianza ciega”, sino como un instrumento de apoyo en la toma de decisiones que, disponible o a su alcance, debe consultar y utilizar, si ello resulta favorable al paciente, so pena de no hacerlo de poder resultar responsable en un caso concreto, habida cuenta de las circunstancias, de los daños causados por incumplimiento de este deber. Debe consultar, y acaso adoptar, decisiones el profesional apoyándose o auxiliándose de los datos de salida que arroje un sistema de IA del que se prevale v.gr, en su función diagnóstica o en cirugía de precisión, pero también como veremos está obligado a controlar y supervisar en lo posible su funcionamiento, salvo que se trate de sistemas autónomos. Estas herramientas pueden ser proactivas a las acciones de los profesionales sanitarios, como los sistemas de predicción de la probabilidad de eventos adversos o de comparación de resultados que modifican los criterios de asistencia⁷⁰.

Con distintos niveles de autonomía, es capaz un sistema de IA de inferir de la información de entrada (“inputs”) que recibe, determinada información de salida (“outputs”)⁷¹ consistente en predicciones, elaboración de

⁷⁰ BENAVENT NÚÑEZ, D. COLOMER MASCARÓ, J. et al, *Inteligencia Artificial y decisiones clínicas: cómo está cambiando ello comportamiento médico*, Fundación Gaspar Casal, 2020, p. 19 citado por GIL MEMBRADO, C. *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Reus, Madrid, 2023, p. 171.

⁷¹ La OCDE ha presentado un “Memorandum explicativo de la definición actualizada de los sistemas de IA” (*Explanatory Memorandum on the updated OECD definition of an AI system*), para ayudar a interpretar la IA en la práctica. Vid. FERNÁNDEZ HERNÁNDEZ, C. Ciberderecho “La OCDE explica el contenido de su definición actualizada de los sistemas de Inteligencia Artificial”, Diario La Ley 06/03/2024, disponible: <https://diariolaley.laleynext.es/dll/2024/03/07/la-ocde-explica-el-contenido-de-su-definicion-actualizada-de-los-sistemas-de-inteligencia-artificial>

Por autonomía de un sistema de IA se entiende el grado en que un sistema puede aprender o actuar sin intervención humana. La supervisión humana puede producirse en cualquier fase del ciclo de vida del sistema de IA: la recopilación y tratamiento de datos, su desarrollo, la verificación, la validación, el despliegue o el funcionamiento.

contenidos, emisión de recomendaciones o adopción de decisiones. La literatura médica abunda en publicaciones científicas que reflejan resultados muy relevantes de la IA en el ámbito médico: con carácter ejemplificativo estos sistemas ayudan a eliminar el ruido de las imágenes clínicas, consiguiendo mayores niveles de precisión a la hora de detectar patologías o tumores; en lo relativo al pronóstico de enfermedades, se aplican hoy herramientas capaces de predecir la progresión de una enfermedad o evaluar la posibilidad de reingreso del paciente; instrumentos laparoscópicos avanzados y robots quirúrgicos permiten realizar cirugías de precisión con mejores resultados que el cirujano humano y considerable reducción de fallos y errores; en el campo de la ómica personalizada se combinan biosensores de ritmo cardíaco, actividad, respiración y patrones de sueño para formular recomendaciones sobre la calidad de vida o elaborar planes personalizados de salud.

Debe tenerse en cuenta que algunos sistemas de IA pueden generar resultados sin que éstos hayan sido descritos explícitamente como objetivos del sistema de IA y sin instrucciones específicas de un humano. En su virtud, el sistema modifica su comportamiento mediante la interacción directa con los datos de entrada antes o después de su despliegue.

Los sistemas de IA pueden entrenarse una vez, periódica o continuamente y funcionan deduciendo patrones y relaciones en los datos. Gracias a este entrenamiento, algunos sistemas de IA pueden desarrollar la capacidad de realizar nuevas formas de inferencia no previstas inicialmente por sus programas. Las entradas se utilizan tanto durante el desarrollo como después de la implantación del sistema de IA. Pueden adoptar la forma de conocimientos, reglas y código que el ser humano introduce en el sistema durante el desarrollo, o de datos. Además, tanto las personas como otras máquinas pueden aportar información al sistema. Las aportaciones también las utiliza un sistema en funcionamiento, por ejemplo, para deducir cómo generar resultados. Las entradas pueden incluir datos relevantes para la tarea que se va a realizar o adoptar la forma de, por ejemplo, una pregunta del usuario o una consulta de búsqueda.

El concepto de “inferencia” se refiere generalmente a la etapa en la que un sistema genera una salida a partir de sus entradas, normalmente después de su despliegue. Cuando se realiza durante la fase de construcción, la inferencia, en este sentido, se utiliza a menudo para evaluar una versión de un modelo, en particular en el contexto del aprendizaje automático. En el contexto del Memorandum, debe entenderse que “inferir cómo generar salidas” se refiere también a la fase de construcción del sistema de IA, en la que se obtiene un modelo a partir de entradas/datos. La(s) salida(s) generada(s) por un sistema de IA suele(n) reflejar las distintas funciones que desempeñan los sistemas de IA. Los resultados de los sistemas de IA suelen pertenecer a las categorías generales de *recomendaciones*, *predicciones* y *decisiones*. Estas categorías corresponden a diferentes niveles de participación humana, siendo las “decisiones” el tipo de salida más autónomo (el sistema de IA afecta directamente a su entorno o dirige a otra entidad para que lo haga) y las “predicciones” el menos autónomo. Debe resaltarse, en este sentido, que el término “predicción” no significa necesariamente realizar una conjetura sobre el futuro, pues puede significar simplemente hacerla sobre un valor desconocido (la salida o “outputs”) a partir de valores conocidos suministrados al sistema (la entrada o “inputs”), como predecir con auxilio en las imágenes clínicas más avanzadas que una región de píxeles en una radiografía es un tumor, lo cual es distinto a “recomendar” una línea de actuación en este caso, o por supuesto a adoptar una decisión, pues “decidir” en última instancia corresponde al médico o equipo médico responsable de la intervención (en términos de la 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica “médico responsable”).

Y es que las implicaciones del desarrollo de la IA y de la robótica en el ámbito de la salud son innegables: el robot es más preciso que el humano, lo que se traduce en la posibilidad de auxiliar en intervenciones de cirugía de alta precisión; es capaz de gestionar en su memoria cantidades de datos inasumibles para un cerebro humano; presenta grandes ventajas tanto a la hora de efectuar diagnósticos como en la labor de pronóstico y en el tratamiento de enfermedades; no teniendo agenda que atender, se halla siempre disponible para el usuario o paciente en función de lo programado, permitiendo reducir costes y prestar una atención individualizada en tiempo real. Lo cual resulta especialmente útil en caso de personas dependientes o con alguna discapacidad: hay estudios que acreditan que reducen la depresión y la soledad de las personas. Además de preciso y eficiente, el robot tiene infinita paciencia, ayudando a profesionales y familias a acompañar y proveer de cuidados a personas ancianas y a comunicarse con niños y niñas con trastornos del espectro autista o que padecen enfermedades raras.

En lo que se refiere a la función diagnóstica, además de los SCA o sistemas de preevaluación de síntomas que ayudan al profesional médico en su función de triaje de enfermedades, los algoritmos mejoran el diagnóstico del cáncer⁷² con el procesamiento y la interpretación de imágenes: el tratamiento conjunto de imágenes médicas permite a los dermatólogos realizar un mejor diagnóstico, detectando hasta el 95% de los cánceres de piel⁷³. La IA reconoce patrones complejos, eliminando el ruido de las imágenes y permitiendo el manejo de modelos tridimensionales⁷⁴. Un sistema de auxilio al radiólogo puede predecir de la combinación de datos agregados (“big data”) que una región de píxeles en una imagen médica digitalizada (texto, imagen, audio y vídeo son contenidos que puede proporcionar la IA generativa) es (o no es) un tumor cancerígeno, pudiendo recomendar una u otra línea de acción al médico o incluso (sólo en el nivel teórico, no en el normativo tras el RIA, por la necesidad de supervisión de los robots) decidir una terapia o tratamiento en un caso clínico concreto.

La robótica en servicios sanitarios de urgencias permite a las unidades de emergencias diagnosticar paradas cardíacas y otras dolencias, incluso mediante el análisis de la voz de la persona que llama. También en las UCI, la robótica se emplea para desinfectar espacios mediante luz ultravioleta (“Assum”) o des-

⁷² En el ámbito oncológico, entre otras muchas aplicaciones, la IA permite a los radiólogos detectar tumores con precisión, al comparar en tiempo real radiografías con gran cantidad de datos médicos.

⁷³ GIL MEMBRADO, C. “Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el Derecho” en GIL MEMBRADO, C. (Dir.), *Bioderecho y Retos*, Dykinson, 2022, pp. 357 a 398.

⁷⁴ GIL MEMBRADO, C. *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Reus, Madrid, 2023, p. 34.

plazándose para atender a pacientes que requieren un seguimiento continuo y a la vez un control remoto (permitiendo al médico efectuar simultáneamente el seguimiento de varios pacientes).

En lo que respecta a la medicina quirúrgica de precisión, dado que la actividad médica debe estar en última instancia supervisada por un profesional en atención a la normativa reguladora de las profesiones sanitarias y el RIA, no está permitida la intervención autónoma, sin supervisión y control humano, de los denominados “robots quirúrgicos”, si bien los brazos quirúrgicos de precisión son utilizados desde hace tiempo⁷⁵ con indudables ventajas en intervenciones técnicamente complejas. Así, el robot “*Da Vinci*” mejora la precisión del médico a la vez que es mínimamente invasivo en cirugías de gran complejidad. Recibe las órdenes del cirujano reproduciendo los movimientos realizados por éste, por lo que carece de autonomía y necesita una orden para proceder. Sus puntos fuertes son la precisión, la seguridad y la mínima invasión, lo que se traduce en una más rápida recuperación y un menor plazo de hospitalización del paciente, la intervención resulta menos traumática y la recuperación menos dolorosa. El cirujano mejora su precisión, destreza y adquiere una visión más completa, clara y nítida, disminuyendo su fatiga, y ello redundando en unos mejores resultados⁷⁶. Al margen de la cirugía laparoscópica, también son de este tipo los robots usados para realizar cateterismos cardíacos, que cuentan con un sensor de IA, que por medio de un algoritmo, localizan en la válvula cardíaca, la fisura o la obstrucción en la arteria⁷⁷. Nuevos y desarrollados sistemas robóticos facilitan ya hoy la inserción de implantes cocleares a personas sordas o con pérdidas auditivas graves: en este tipo de implantes, las aplicaciones robóticas posibilitan la colocación a través de las delicadas y diminutas estructuras de la cóclea con gran precisión y estabilidad⁷⁸.

También se utilizan hoy aplicaciones de IA y robots en la rehabilitación de pacientes: entre muchas otras aplicaciones médicas y de fisioterapia, en

⁷⁵ Desde 1985, en que se realizó el primer procedimiento neuroquirúrgico asistido por el robot industrial PUMA para introducir una guía en una biopsia cerebral. Posteriormente, los robots asistenciales en quirófano, como “AESOP” para cirugía endoscópica, controlado por voz; “NeuroMate”, para realizar terapias de estimulación cerebral profunda, neuroendoscopia, estereoelectroencefalografía, biopsias e investigación; el “DaVinci” que facilita una visión 3D con un aumento de hasta diez veces, eliminando el temblor fisiológico del cirujano humano, que es utilizado en intervenciones de urología, cirugía oral y maxilofacial, pediátrica, torácica y cardíaca; “Robodoc” para cirugía ortopédica; “Acrobot” para cirugía de rodilla y “CyberKnife” para el tratamiento no invasivo de tumores. GIL MEMBRADO, C. *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Reus, Madrid, 2023, pp. 39 a 41.

⁷⁶ Vid. <https://www.intuitive.com/en-us/products-and-services/da-vinci>

⁷⁷ GIL MEMBRADO, C. “Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el Derecho” en GIL MEMBRADO, C. (Dir.), *Bioderecho y Retos*, Dykinson, 2022, p. 377.

⁷⁸ https://www.consalud.es/tecnologia/tecnologia-sanitaria/sistema-robotico-facilita-insercion-implantes-cocleares_104349_102.html

el tratamiento posterior a accidentes de circulación mediante ejercicios físicos, o enfermedades cerebro-vasculares. En el campo de la salud mental, ya hay chabots y robots que sirven de psicoterapeutas virtuales y pueden ayudar en el tratamiento de problemas psicológicos como la ansiedad o la depresión (Ebers⁷⁹), ofreciendo herramientas para trabajar sus síntomas o desarrollar habilidades sociales.

Los robots también pueden desempeñar una importante función de apoyo a las personas ancianas y dependientes⁸⁰, tanto en lo relativo a su movilidad como a su seguridad personal y en el mantenimiento de su salud física y psíquica⁸¹. En relación a la asistencia, combinando tecnologías como la localización GPS, IA y sensores corporales en tejidos inteligentes, es hoy posible predecir comportamientos de personas mayores, e incluso detectar emociones a través del reconocimiento facial. Gil Membrado cita⁸² a varios robots sanitarios con función de asistencia en la dispensación de medicación a pacientes y ancianos: *Pillo* reconoce voces, rostros y ofrece a tiempo la medicación que guarda en un compartimento, *Gower* realiza el suministro, mezcla y dispensación de fármacos con la finalidad de minimizar el error humano, calculando las dosis para quimioterapia en los gravesos tratamientos oncológicos. Un caso curioso: el robot *Xiaoyi* superó el examen para ejercer la medicina al aprobar, según su desarrolladora, la “*National Medical Licensing Examination*” en China: instrumento de apoyo a los profesionales revisando rápidamente historias clínicas de los pacientes, tras lo que puede llegar a sugerir un tratamiento u otro⁸³.

⁷⁹ “*The Top 12 Healthcare Chatbots*”, Medical Futurist, 2021. <https://medicalfuturist.com/top-12-health-chatbots/> citado por EBERS, M. ¿Terapia sin terapeutas?, en LUQUIN BERGARECHE, R (Dir.) *Servicios privados de telemedicina y Salud Digital: retos e implicaciones jurídicas*, Tirant lo Blanch, 2024, pp.32 y siguientes.

⁸⁰ EBERS, M. “¿Terapia sin terapeutas?”, en LUQUIN BERGARECHE, R (Dir.) *Servicios privados de telemedicina y Salud Digital: retos e implicaciones jurídicas*, Tirant lo Blanch, 2024, pp.32 a 38.

⁸¹ Los denominados “robots de servicio” pueden “ayudar y vigilar a los ancianos midiendo la presión sanguínea o los niveles de oxígeno, detectando emergencias y realizando llamadas de urgencia, haciendo videollamadas a familiares o amigos, guardando objetos importantes como llaves o carteras, o recordando a los usuarios que acudan a sus citas, tomen sus medicamentos, alimentos o líquidos. Muchos robots también pueden suministrar a los ancianos sus medicamentos o darles de comer, bañarlos y lavarlos. Para ayudar a tratar la demencia, algunos robots son capaces de proporcionar estimulación cognitiva y recordatorios. (...) Además, los robots también pueden servir de compañía a la persona mayor y mantener diálogos personalizados o jugar con ella. Los robots con aspecto de animales, como Paro o AIBO, que se parecen a perros o focas, son una alternativa a las mascotas y acompañan a los mayores en su vida diaria”. EBERS, M. *Ob. cit.* p.37.

⁸² AVILA TOMAS, J.F.; MAYER PUJADAS, M.A.; QUESADA VARELA, V.J.; “La inteligencia artificial y sus aplicaciones en medicina: importancia actual y aplicaciones prácticas, *Atención Primaria*, vol. 53, n.º.1, 2020, pp. 83-84; RAMON FERNÁNDEZ, F., “La inteligencia artificial y la medicina: médicos robots o robots médicos?”, *Revista Chilena de Derecho y Tecnología*, vol. 10, n.º. 1, 2021, p. 334 citando a LEON RODRIGUEZ, H., “Sistema macro & micro robótico para aplicaciones médicas”, *Revista de Tecnología*, vol. 16, n.º 2, pp. 104-113. Citados por GIL MEMBRADO, C. *ob. cit.* p. 366.

⁸³ https://www.consalud.es/saludigital/103/xiaoyi-el-robot-que-pasa-consulta-en-china-tras-aprobar-medicina_48531_102.html

Como veremos, puede tratarse de IA simple o “débil” o, más frecuentemente en el campo de la salud de IA “profunda” basada en el aprendizaje automático de las redes neuronales (“deep learning”) que diseñan modelos predictivos desde un conjunto inicial de datos, identificando patrones y correlaciones a partir de grandes cantidades de “data”, realizando inferencias y haciendo predicciones basadas en dicha información. Los sistemas de IA en salud pueden llegar a simular a través de modelos matemáticos modelos biológicos neuronales y, dada su capacidad de extraer patrones complejos, tienen un gran potencial para la predicción de resultados⁸⁴, pudiendo operar modo autónomo al aprender el sistema del entorno, arrojando como “outputs” decisiones o recomendaciones cuya trazabilidad escapa de la supervisión humana: en este caso se pone en cuestión la transparencia y explicabilidad de estos sistemas en ámbitos como la salud que afectan a derechos (vida, integridad física, salud, intimidad) e intereses fundamentales de las personas.

No hablamos de ciencia ficción: la prestigiosa publicación científica “The Lancet” ha publicado recientemente que investigadores británicos han desarrollado un sistema de redes neuronales profundas de código abierto “X-Rayda”⁸⁵ que permite realizar lecturas completas de radiografías de tórax empleando la IA como herramienta de triaje para comparar las pruebas con un enorme volumen de datos. El sistema es de libre acceso y está entrenado con grandes conjuntos de datos para que los profesionales (escasos en esta especialidad) puedan cotejarlos con sus propias pruebas de imagen⁸⁶.

A pesar de las ventajas que ofrece la IA, no debe el profesional médico actuar “como mera correa de transmisión”⁸⁷ de las inferencias de estos sistemas, lo que llevaría a decisiones automatizadas, sino que les corresponde a adoptar

⁸⁴ BENAVENT NÚÑEZ, D. COLOMER MASCARÓ, J. et al, *Inteligencia Artificial y decisiones clínicas: cómo está cambiando ello comportamiento médico*, Fundación Gaspar Casal, 2020, p.21. Ver también BUSTINCE SOLA, H., “Caminos hacia la superinteligencia”, en LLEDÓ YAGÜE, F., BENÍTEZ ORTÚZAR, I., MONJE BALMASEDA, O., (dirs.) *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, 2021, p. 560.

⁸⁵ El algoritmo comprueba automáticamente una radiografía de tórax para detectar la presencia de 37 hallazgos radiológicos anormales en tiempo real. Para ello, en el proyecto se desarrollaron redes neuronales de código abierto para clasificar los resultados de miles de imágenes e informes de radiografías de tórax procedentes de seis hospitales del Reino Unido: nada menos que 2,5 millones, tomadas a lo largo de un periodo de 13 años. Como resultado, un sistema de IA capaz de detectar de forma integral diferentes tipos de anomalías en las pruebas de rayos X de tórax mediante el entrenamiento de un algoritmo con miles de datos procedentes de bases de datos de rayos X.

⁸⁶ CID, YASHIN DICENTE et al., “Development and validation of open-source deep neural networks for comprehensive chest x-ray reading: a retrospective, multicentre study”, *The Lancet Digital Health*, Volume 6, Issue 1, e44 - e57. Disponible en: [https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(23\)00218-2/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(23)00218-2/fulltext)

Vid. Chester the AI Radiology Assistant. Disponible en: <https://mlmed.org/tools/xray/>

⁸⁷ GIL MEMBRADO, C., ob. cit, p. 175.

la última decisión, para lo cual resulta necesario que comprendan la lógica, al menos, del razonamiento logarítmico que conduce a la información de salida o “output” materializada en diagnósticos, pronósticos, recomendaciones o decisiones sobre enfermedades o patologías de sus pacientes⁸⁸. Adoptar “la última decisión” puede ser, en un caso concreto, la de no utilizar la IA e ignorar la decisión del sistema: para ello es necesario que pueda participarse en el diseño del mismo y en el seguimiento de todas sus fases, supervisando desde un punto de vista dinámico, como afirma De Miguel, no sólo los datos con los que se cuenta antes de permitir su comercialización sino también realizando un seguimiento “ex post” a su introducción en el mercado, certificando que no se han introducido sesgos, voluntaria o involuntariamente, lo cual es especialmente relevante, sobre todo en sistemas algorítmicos de prognosis que implican actividades de predicción⁸⁹.

Las oportunidades de los sistemas de IA en el ámbito de la salud son innegables, pero desde el punto de vista jurídico deben ponerse también sobre la mesa, para conjurarlos o minimizarlos en lo posible, sus riesgos. Sólo de este modo, dotada de un marco ético y normativo armonizado, la IA gozará de confiabilidad para usuarios profesionales y no profesionales más allá de la fuerza inherente a la eficiencia del algoritmo, lo cual resulta esencial para su implementación práctica en un ámbito, como la salud, que afecta derechos fundamentales de las personas.

2. LA PREVENCIÓN DE LOS RIESGOS DE LA INTELIGENCIA ARTIFICIAL EN SALUD A LA LUZ DEL REGLAMENTO (UE) 2024/1689 DE 13 DE JUNIO DE 2024, POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE IA (RIA)

2.1. PRIMER MARCO REGULATORIO EUROPEO DE LA IA

En un contexto como el actual de desarrollo tecnológico, la aprobación de un primer marco regulatorio europeo de la inteligencia artificial ha pretendido lograr un punto de equilibrio entre el avance tecnológico y la salvaguar-

⁸⁸ Al principio de “autonomía supervisada de los robots” se refería ya la **Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL))** y se refuerza en el reciente RIA.

⁸⁹ DE MIGUEL BERIAIN, I. “Medicina personalizada, algoritmos predictivos y utilización de sistemas de predicción automatizados en asistencia sanitaria: problemas éticos”, *Dilemata*, n° 30, 2019, p.96.

da de derechos individuales. El desafío era (y es” monumental y la necesidad regulatoria, urgente, en un contexto de vertiginosos avances que conllevan grandes oportunidades a la par que no pocos riesgos). Pese al carácter bifronte de una unión política que, no deja de ser antes económica, lo cierto es que, en este ciclo histórico de inflexión que estamos viviendo, la normativa comunitaria había alcanzado elevadas cotas de protección de la privacidad personal y, en general, salvaguarda de derechos iniduales. La irrupción de la IA ha supuesto importantes desafíos que afectan tanto a sociedad civil y mercado (empresas y consumidores) como a las mismas democracias (ciudadanos).

En el ámbito que nos ocupa además de a los derechos de la personalidad como la garantía de protección de los datos personales, la implementación de sistemas de IA afecta a las personas en su condición de consumidores y usuarios pero también, y sobre todo, de pacientes. De ahí la urgencia de una respuesta regulatoria armonizada a una realidad compleja que compromete variadas necesidades e intereses de actores públicos y privados.

El pasado 1 de agosto de 2024 entró en vigor⁹⁰ el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial, en adelante RIA), que tiene por objeto fomentar el desarrollo y la implantación responsables de la IA en la Unión Europea. El objetivo de esta norma es mejorar el funcionamiento del mercado interior y promover la adopción de una IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta (...), frente a los efectos perjudiciales de los sistemas de IA así como prestar apoyo a la innovación⁹¹.

La contenida en el punto 1 del actual art. 3 (68 definiciones en total) entiende por «sistema de IA» “un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones

⁹⁰ A partir de esa fecha, será plenamente aplicable veinticuatro meses después, excepto para ciertas disposiciones específicas: las prohibiciones de prácticas prohibidas: seis meses después; los códigos de práctica nueve meses después; las normas de IA de uso general, incluida la gobernanza: doce meses después y las obligaciones para sistemas de alto riesgo, treinta y seis meses después.

⁹¹ Propuesto por la Comisión en abril de 2021 y aprobado por el Parlamento y el Consejo en diciembre de 2023, la norma, de aplicación general y directa en los estados miembros, aborda algunos posibles riesgos para la salud, la seguridad y los derechos fundamentales de los ciudadanos, proporciona a los desarrolladores e implementadores requisitos y obligaciones en relación con usos específicos de la IA, reduciendo al tiempo las cargas administrativas y financieras para las empresas.

o decisiones, que pueden influir en entornos físicos o virtuales”. La definición⁹² es amplia y abarca casi todos los programas informáticos y robots con IA: desde simples chatbots, dispositivos de preevaluación de síntomas, software de dispositivos médicos, medidores de glucosa en sangre con IA, o sistemas inteligentes de predicción de episodios de migraña o asma, hasta complejos software de análisis de imágenes médicas en radiología.

Si bien el RIA a nuestro juicio merece de entrada una valoración positiva, en cuanto favorece el desarrollo tecnológico y el crecimiento económico de la UE a través de una legislación común, no puede obviarse que la norma adolece, desde el punto de vista formal, de falta de sistemática y desde el material-sustantivo, de un insuficiente grado de profundidad y detalle a la hora de regular cuestiones de tanto calado como las singularidades y riesgos inherentes a ciertos sistemas de IA. Afectando el desarrollo de esta tecnología a un ámbito de la actividad humana tan extenso (democracias, mercados, sociedad civil) como sensible (compromete derechos e intereses públicos y privados), la opción del legislador comunitario por los “sandboxes” como arenas o campos de prueba o experimentación de la implementación de estas tecnologías ya apunta, de algún modo, a la aceptación como inevitable de la incompletitud de este primer ecosistema regulatorio.

2.2. RIESGOS Y SALUD: LA AMBIGÜA DEFINICIÓN DE LOS SISTEMAS IA DE ALTO RIESGO

El de la salud es uno de esos ámbitos que exigirá un mayor grado de concreción normativa en los futuros desarrollos y complementos legislativos previstos ya en el mismo reglamento aprobado. Ya de entrada parece poco acertada y ciertamente cuestionable la opción del legislador por un marco normativo horizontal, en lugar de hacerlo por normativas sectoriales que hubieran permitido incorporar singularidades de cada ámbito de actividad (políticas públicas y democracia, salud, etc.). La pretendida armonización ante un “tsunami” como el que representa la IA, resulta a la postre deficiente: de ello da fe la necesidad de utilizar extensos anexos complementarios y del frecuente recurso a lo largo de su articulado a la técnica de las remisiones a marcos normativos que contienen definiciones y regulaciones de difícil articulación con la actual regulación de la IA: como el de protección de datos personales, la regulación de productos sanitarios y de productos defectuosos, el de tutela

⁹² No se identifica ya sistema de IA con “software” ni se remite a tecnologías o métodos concretos listados en un Anexo (como en el último borrador). Los sistemas de IA se diferencian de los que no lo son por sus funcionalidades y capacidades: (i) autonomía, (ii) capacidad de adaptación y (iii) generación de resultados de salida en base a información de entrada recibida.

de consumidores y usuarios o, singularmente en lo que respecta a la digitalización de la salud, los recientes relativos a los mercados y los servicios digitales.

La norma, de aplicación general y directa, dispone en su art. 1 que su objeto es mejorar el funcionamiento del mercado interior y promover la adopción de una IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales (...), frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación. Para ello, establece normas armonizadas (así se pretende) para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la UE, prohibiciones de determinadas prácticas de IA, requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas y normas armonizadas de transparencia aplicables a determinados sistemas de IA, entre otras (art. 2). A los sistemas clasificados “de alto riesgo” de conformidad con el art. 6, apartados 1 y 2, y asociados a productos regulados por los actos legislativos de armonización de la Unión indicados en la sección B del anexo I, únicamente se les aplicarán los arts. 11 (documentación técnica), 12 (conservación de registros), 13 (transparencia y comunicación de información a los responsables del despliegue)⁹³, 14 (supervisión humana⁹⁴) y art. 15 (precisión, solidez y ciberseguridad⁹⁵) .

⁹³ Regulación de la “Transparencia y comunicación de información a los responsables del despliegue”.

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.

2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue (...).

⁹⁴ El art. 14 RIA se refiere a la necesidad de supervisión humana de estos sistemas:

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

2. El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos establecidos en la presente sección.

3. Las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo, y se garantizarán bien mediante uno de los siguientes tipos de medidas, bien mediante ambos: a) las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en b) medidas que el proveedor defina antes de la introducción del sistema de IA de alto

riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue; c) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1, 2 y 3, el sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada a: entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados, b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión, c) interpretar correctamente los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere; d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura

5. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación.

El requisito de la verificación por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.

⁹⁵ El art. 15 regula la "Precisión, solidez y ciberseguridad de los sistemas de IA de alto riesgo:

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.

2. Para abordar los aspectos técnicos sobre la forma de medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 y cualquier otro parámetro de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y organizaciones pertinentes, como las autoridades de metrología y de evaluación comparativa, fomentará, según proceda, el desarrollo de parámetros de referencia y metodologías de medición.

3. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión de dichos sistemas, así como los parámetros pertinentes para medirla.

4. Los sistemas de IA de alto riesgo serán lo más resistentes posible en lo que respecta a los errores, fallos o incoherencias que pueden surgir en los propios sistemas o en el entorno en el que funcionan, en particular a causa de su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.

Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que se elimine o reduzca lo máximo posible el riesgo de que los resultados de salida que pueden estar sesgados influyan en la información de

Son indudables los beneficios que la IA (v.gr., un SCA o un robot quirúrgico como el “DaVinci”) proporcionan en el ámbito de la salud digital, pero no deben olvidarse los riesgos que pueden materializarse en daños que es necesario evitar o minimizar. Por ello, y afectando a derechos intereses jurídicos especialmente sensibles y merecedores de los más altos niveles de protección (vida, integridad física, salud, privacidad personal...), estos sistemas deben cumplir, como veremos, elevados estándares de transparencia e información, explicabilidad, garantías de privacidad y evitación de sesgos.

No creo que pueda afirmarse, más bien al contrario, que en el ámbito de la salud el empleo de la IA como “auxilio” del médico humano incrementa “de facto” el riesgo de producción de daños. Ahora bien: una cosa es que no se incrementen los riesgos y otra que, materializado un daño como concreción de un riesgo, resulte necesario determinar quién responde del mismo (fabricante, diseñador del sistema, “responsable del despliegue”⁹⁶) y con base a qué fundamento jurídico.

entrada de futuras operaciones (bucles de retroalimentación) y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos adecuadas.

5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su funcionamiento aprovechando las vulnerabilidades del sistema.

Las soluciones técnicas encaminadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo serán adecuadas a las circunstancias y los riesgos pertinentes.

Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo.

⁹⁶ Los “responsables del despliegue” en el ámbito que nos ocupa son los usuarios profesionales de estos sistemas y dispositivos: esto es, los profesionales médicos. Los centros de salud y centros hospitalarios públicos o privados son los garantes de la supervisión de estos sistemas de IA, robots y dispositivos de los que se prevalecen los profesionales sanitarios que en ellos prestan servicios (igualmente las plataformas de telemedicina que incorporen estos sistemas, tanto frente a los facultativos que reclutan como frente a los usuarios de estas plataformas). Son ellos (en el caso de servicios públicos de salud, las administraciones públicas) los encargados de poner en práctica las instrucciones de uso que garanticen “un nivel adecuado de alfabetización, formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas (C. 91 RIA), por encontrarse “en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos (...) al tener un conocimiento más preciso del contexto de uso y de las personas o los grupos de personas que probablemente se vean afectados, entre los que se incluyen grupos de personas vulnerables y (...) también desempeñan un papel fundamental a la hora de informar a las personas físicas y, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, deben, en su caso, informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman (C. 93).

Dejando a un lado cuestiones específicas como las relativas al riesgo para la protección de los datos personales, la IA no añade un plus de peligro al ejercicio de una profesión, la médica, que, ya de por sí, implica riesgos⁹⁷ para la vida y la salud de los pacientes y en la que el profesional responde con criterios culpabilísticos (otra cosa es que en beneficio del resarcimiento del daño causado a la víctima -principio “pro damnato”-, se articulen expedientes que permitan aliviar el “onus probandi”, pues debe aportar la prueba aquella parte que se halle en mejores condiciones de hacerlo. Así lo prevé el ordenamiento procesal español en el art. 217.7 LEC y lo contempla en numerosos pronunciamientos la jurisprudencia en materia de responsabilidad sanitaria cuando recurre a la aplicación de la máxima “res ipsa loquitur”⁹⁸, de la doctrina del daño desproporcionado⁹⁹, la distribución dinámica de la prueba¹⁰⁰ o mediante el empleo de presunciones¹⁰¹.

En definitiva, el avance que supone la IA no impide la posible materialización de daños que obedecen a orígenes y causas imputables a distintos agentes: defectos de fabricación o diseño (en su caso, sujetos a la legislación de productos defectuosos), error en la programación de estos dispositivos, fallos de ciberseguridad por hackeos en la red, error de los denominados “responsables del despliegue” en el tratamiento de los datos de salida (“outputs”) u otros supuestos de negligencia profesional en el manejo y supervisión de estos sistemas.

⁹⁷ En algunos casos inevitables en cuanto debidos a lo que el Tribunal Supremo denomina “zonas oscuras de los cursos causales de la vida humana” (STS de 10 de abril de 2.001).

⁹⁸ Se trata de una presunción en virtud de la cual se permite deducir, de un hecho probado y evidente, la existencia de culpa. Los requisitos son: a) Que el hecho evidente o probado debe encontrarse entre los que normalmente no ocurren sin negligencia (no es suficiente la mera rareza o anormalidad); b) La negligencia debe aparecer como la única causa posible; y c) El profesional al que se imputa la responsabilidad debe tener control del paciente y del instrumental (en este caso del sistema de IA). d) Inexistencia de contribución causal o culposa por parte del paciente o de un tercero. Entre otras, SSTs 12 de julio de 1998, 9 de diciembre de 1998 y 24 de marzo de 2001.

⁹⁹ La doctrina de la “faute virtuelle” o su equivalente del “daño desproporcionado” se limita a deducir la negligencia de la anormalidad del resultado dañoso con lo que es usual comparativamente. Se deduce la culpa a partir de la existencia de un nexo de causalidad entre la intervención y su anómalo resultado: el daño. SSTs 30 de enero 2.003 y 19 de mayo de 2006.

¹⁰⁰ Consiste en repartir la carga de la prueba de manera que se obligue a aportar cada una de las pruebas aquella parte que se encuentre en mejores condiciones de hacerlo. Responde a la concepción del análisis económico del derecho: está en mejores condiciones probatorias aquel sujeto procesal que puede aportar las pruebas de manera más eficiente, ya sea por tener la información o el soporte documental de esta (el que es capaz de acceder a dicha prueba con el coste más barato posible). Entre otras, SSTs 6 de febrero de 2001, 23 de diciembre de 2002, 14 de febrero de 2007.

¹⁰¹ Se trata de la inferencia lógica de un hecho demostrado de otro, entre los que hay un “enlace preciso y cierto según las reglas del criterio humano” (SSTs 12 de febrero de 1990 y 12 de febrero de 2001).

La regulación de los sistemas de IA de alto riesgo del RIA es la siguiente:

De conformidad con la remisión de su anexo I al RPS, se considerará el sistema de IA de alto riesgo cuando “a) *esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I*¹⁰², o que el propio sistema IA sea uno de dichos productos; y b) (...) *deba someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I*”.

Son sistemas de alto riesgo los productos sanitarios que deban someterse a evaluación de conformidad ex RPS: esta es la norma general. La excepción a esta regla, está redactada en forma deliberadamente ambigua. Así, un sistema de IA de este tipo “(...) *no se considerará de alto riesgo si no plantea un riesgo importante*¹⁰³ *de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, en particular al no influir sustancialmente en el resultado de la toma de decisiones, tenga por objeto llevar a cabo una tarea de procedimiento limitada, mejorar el resultado de una actividad humana previamente realizada; detectar patrones de toma de decisiones (...) y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III*” (art. 6 RIA).

En definitiva, es considerado “sistema de IA de alto riesgo” con arreglo al RIA por la posibilidad de influir en la toma de decisiones sobre la salud y los derechos fundamentales de las personas si tiene la consideración de “producto sanitario” con arreglo a lo previsto en el RPS (dependiendo en cierta medida, como se ha visto, del fabricante -criterio subjetivo- determinar la “finalidad prevista”¹⁰⁴ de un sistema o dispositivo): “*todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fa-*

¹⁰² Entre los que se encuentran los productos sanitarios (RPS).

¹⁰³ Causa perplejidad la indeterminación normativa de la adjetivación: no se considerará de “alto riesgo” si no plantea un riesgo “importante” de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas: el legislador comunitario pretende autoexplicarse en el mismo precepto indicando que la importancia de un determinado “riesgo” de una IA viene dada por su capacidad de influencia en el resultado de la toma de decisiones (a la postre, humanas). Si influye sustancialmente en el resultado de la adopción de decisiones relativas a la salud, la seguridad o los derechos fundamentales de las personas físicas, lo cual es así en la generalidad de los casos, la IA plantea un riesgo importante, ergo deberían considerarse en dicha categoría los sistemas de IA en salud salvo excepciones (v.gr. los chatbots o los SCA con finalidad meramente informativa al paciente-usuario siempre que no sean productos sanitarios), con los consiguientes efectos.

¹⁰⁴ No es la misma la definición de lo que es la “finalidad prevista” de un producto sanitario que incorpora IA el RPS que en la LIA: a efectos de esta norma, «finalidad prevista» es el uso para el que “un proveedor” concibe un sistema IA, incluidos el contexto y las condiciones de uso concretos,

bricante a ser utilizado en personas, por separado o en combinación”. Debiendo para ello ser utilizado con finalidad médica específica de “diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad; diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad; investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico; obtención de información mediante el examen “in vitro” de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos, y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos”.

No será de alto riesgo el robot o sistema IA en el ámbito sanitario, con los consiguientes efectos, si no plantea un riesgo “importante” de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas. Entendiéndose, en particular, que no existe tal relevancia (esto es, un elevado grado de riesgo o probabilidad de materializarse tal peligro en daño efectivo) cuando la aplicación de la IA no influya “de forma sustancial” en el resultado de la toma de decisiones o lleve a cabo una tarea de procedimiento limitada, mejore el resultado de una actividad humana previamente realizada o detecte patrones de toma de decisiones (...) y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o llevar a cabo una tarea preparatoria para una evaluación.

Pues bien: en el campo de la medicina será difícil que un riesgo no sea valorado como “relevante” a estos efectos, por la incidencia que las decisiones médicas tienen en la vida, integridad, salud de las personas, o, de modo más amplio, en sus derechos de la personalidad (privacidad, intimidad, dignidad...protegidos a nivel constitucional). Por otra parte, no puede en este ámbito concebirse la IA más que como complemento o instrumento auxiliar, en mayor o menor grado, del profesional médico que es quien en definitiva va a decidir, tanto si se trata de actividad diagnóstica, como pronóstica, de terapia o cura o de rehabilitación del paciente.

Fuera de los casos de las “tareas de procedimiento limitadas” (v.gr. tareas rutinarias como el transportar de equipos dentro de las instalaciones, la entrega de material de cama, el rastreo de suministros, la limpieza y desinfección de superficies contaminadas utilizando luz UV, etc.) o de “detección algorítmica de patrones de toma de decisiones”¹⁰⁵ a las que se refiere el pre-

según la información facilitada por el mismo en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

¹⁰⁵ Como por ejemplo, el análisis de vastas cantidades de datos de pacientes en radiología facilita la identificación de patrones que, de otro modo, no se evidencian al profesional, lo cual permite diagnósticos más precisos y tempranos y precisos en beneficio de los pacientes.

cepto, en lo demás habrá que analizar cada caso para valorar si el auxilio de un sistema de IA influye o puede influir “sustancialmente” en una decisión médica.

Así será en la generalidad de los casos. A tenor de la norma aprobada, los requisitos esenciales de los sistemas de IA de alto riesgo deben evaluarse como parte del procedimiento de evaluación de conformidad del RPS: lo cual implica para el organismo notificado (en nuestro país, la Agencia Española de Supervisión de la IA) que realiza la evaluación la obligación de revisar también los requisitos específicos, que incluyen la creación de un sistema de gestión de riesgos, criterios de calidad para los datos de formación, validación y ensayo en relación con la pertinencia, representatividad, exactitud y exhaustividad para evitar sesgos y discriminaciones; documentación técnica y mantenimiento de registros, información necesaria para evaluar la conformidad con los requisitos pertinentes; disposiciones sobre transparencia e información al usuario para abordar la opacidad de determinados sistemas de IA; obligaciones de supervisión humana que incorporen una herramienta de interfaz humano-máquina para garantizar que los sistemas puedan ser vigilados de manera efectiva por personas físicas y obligaciones relativas a la precisión, robustez y ciberseguridad de los sistemas. Requisitos que, como afirma la doctrina, se hallan redactados de forma excesivamente amplia¹⁰⁶, definiendo los elementos esenciales y dejando la regulación de detalle a las normas elaboradas por los organismos europeos de normalización.

2.3. OBLIGACIONES DE PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE: INFORMACIÓN Y SUPERVISIÓN

Garantizar la trazabilidad del algoritmo es uno de los retos más difíciles a que se enfrentan los sistemas de IA. El deber de transparencia es fundamental, tanto para generar la necesaria confianza en estos sistemas como para que, llegado el caso, pudiera exigirse del “responsable del despliegue” que se prevale de la IA, responsabilidad civil si el riesgo se materializara en daños. Tanto el diseño como el desarrollo del sistema de IA deben ser transparentes y explicables para que los responsables de su despliegue (centros de salud, hospitales, médicos) puedan interpretar y hacer uso correcto de la información de salida de estos sistemas (“outputs”). La trazabilidad implica registrar y documentar las decisiones tomadas por los sistemas, incluyendo una descripción de la recogida y el etiquetado de datos, así como del algoritmo que ha dado

¹⁰⁶ Para un análisis detallado del nuevo marco legislativo en relación con la propuesta de la LIA, véase EBERS, M., “Standardizing AI - The Case of the European Commission’s Proposal for an Artificial Intelligence Act”, *ob. cit.*, pp.321-344.

lugar a una determinada decisión. Como afirma GIL MEMBRADO¹⁰⁷, sólo de este modo, conociendo la explicabilidad del proceso de toma de decisiones algorítmico, es decir, su “lógica decisional”, el perjudicado podría, materializado un daño, impugnar la decisión de forma motivada.

Las obligaciones de los proveedores de IA se enumeran en los arts. 16 a 22 RIA, las de los importadores en el art. 23, los deberes a cargo de los distribuidores en el art. 24, el art. 25 regula las obligaciones a cargo de distintos agentes a lo largo de la cadena de valor, y el art. 26 se refiere en concreto a las obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo, que en particular (núm.1) “adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen”.

Un factor añadido de complejidad viene dado por la opacidad o falta de transparencia de algunos sistemas de IA autónoma (la llamada “caja negra” o “*black box*”). Garantizar en el ámbito de la salud la transparencia en la información suministrada a los profesionales que van a hacer uso de este tipo de dispositivos¹⁰⁸ condiciona directamente el avance de un modelo, el de Salud Digital, que precisa de la confianza de todos los agentes involucrados.

En relación a los sistemas de alto riesgo como son los de IA en salud, el art. 13 RIA se refiere a tales deberes de transparencia y comunicación de información a cargo de proveedores (fabricantes, desarrolladores, diseñadores de los productos) y los que denomina “responsables del despliegue” de la IA, disponiendo la siguiente regulación:

“1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones oportunas previstas en la sección 3.

2.(...) irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue (...).”

¹⁰⁷ GIL MEMBRADO, C. “Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra”, en Derecho de contratos, responsabilidad extracontractual e inteligencia artificial, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024. p. 520-521.

¹⁰⁸ EBERS pone como ejemplo que un sistema de IA puede ser capaz de detectar un delirio inminente en un paciente hospitalizado antes de que los síntomas sean visibles, a pesar de lo cual el mero resultado del sistema de IA - sin información sobre la causalidad o la lógica que subyace a la predicción- puede no ser suficiente para los médicos, ya que tal delirio puede manifestarse de muchas formas, a menudo contradictorias.

Un centro médico u hospitalario o un profesional médico que, en este sentido, hace uso, se prevale o auxilia de una aplicación o sistema de IA en el ejercicio de sus funciones de diagnóstico, terapéutica, quirúrgica o rehabilitadora de la salud del paciente es, a la luz del RIA, “responsable del despliegue” de tal sistema de IA. Este profesional (médico, pero también un fisioterapeuta, un enfermero en el ámbito de sus funciones, etc.) adoptará decisiones que pudieran, en parte, sustentarse o apoyarse en “*inputs*” de entrada (es decir, en información facilitada por la IA) correspondiendo al proveedor (bien al fabricante o, en su caso, al diseñador de una IA -v.gr., un software-) facilitar dichas “instrucciones de uso” con un nivel de transparencia tal que permita a cada parte involucrada cumplir las obligaciones que la norma le impone. Instrucciones de uso que, en cualquier caso, deben contener información no solo correcta, sino también concisa, completa, y clara que sea además “pertinente, accesible y comprensible” para tales profesionales (en principio y como regla general, legos tecnológicos).

Sólo si se cumplen estas condiciones podría derivarse responsabilidad en caso de incumplimiento o cumplimiento defectuoso de las obligaciones del médico, las derivadas de su “*lex artis ad hoc*”, a saber: *cura* del paciente como obligación de medios e información asistencial al paciente (previa al CI) también de estos riesgos tecnológicos, que debe recabarse del paciente¹⁰⁹ y las que se derivan de prevalerse de instrumentos auxiliares de IA en el desempeño de su función que se haya materializado en un daño.

Los deberes de vigilancia y supervisión de estos sistemas corresponden a personas físicas: la normativa exige que los sistemas de IA de alto riesgo se diseñen y desarrollen de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período en que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas: el objetivo será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales cuando no se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible (art. 14 RIA).

Pues bien: ocurre que la regulación de estos deberes difiere de la establecida por el RPS: si bien el RPS no establece explícitamente un deber al fabricante en tal sentido, de sus disposiciones se deriva su obligación de acreditar documentalmente que la seguridad y las prestaciones de los productos sanitarios se adecúan al estado de la técnica en cada caso de teniendo en cuenta su uso previsto¹¹⁰. El Anexo I No. 23(1) RPS exige a los fabricantes proporcionar

¹⁰⁹ Debe conocer estos riesgos para consentir la intervención, si aplicamos lo dispuesto en la LBRAP.

¹¹⁰ En base a estudios que demuestran que algunos sistemas “opacos” de IA como las denominadas “redes neuronales profundas” muestran un grado de precisión y eficiencia notablemente

“información pertinente sobre la seguridad y el funcionamiento para el usuario o cualquier a otra persona, según proceda”, adaptada a “los conocimientos técnicos, la experiencia, la educación o la formación de los usuarios previstos”. La información debe destacar los beneficios clínicos que cabe esperar (Anexo I No. 23.4 RPS) y las características de funcionamiento del producto (Anexo I No. 23.4 (e) RPS), permitiendo así al profesional sanitario verificar si el producto es adecuado (Anexo I No. 23. 4(f) RPS). Al igual que en ámbitos distintos de la salud, resulta problemática la inexistencia de un marco normativo uniforme aplicable a todos los estados miembros¹¹¹ que vaya más allá de las soluciones técnicas a los fabricantes para garantizar el cumplimiento del RPS. La normativa se refiere a seguridad *física* de los dispositivos¹¹², brillando por su ausencia criterios normativos claros relativos a los riesgos que, en el campo de los derechos

superior -se dice- a los sistemas transparentes, algunos expertos abogan por tratar de alcanzar un delicadísimo equilibrio en este punto entre criterios de eficiencia y criterios de seguridad. A diferencia del RIA, que no se centra en los beneficios esperables sino en los riesgos, el RPS permite la asunción de ciertos riesgos como aceptables si se compensan con los beneficios correspondientes (Anexo I No. 4 RPS).

¹¹¹ Para una evaluación crítica del nuevo marco legislativo en el contexto de los sistemas de IA, *vid.* EBERS, M. “Standardizing AI - The Case of the European Commission’s Proposal for an Artificial Intelligence Act”, en DIMATTEO, L. A., PONCIBÒ, C. y CANNARSA, M. (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2022, pp.321-344.

¹¹² La normativa sobre responsabilidad derivada de productos defectuosos está constituida por la Directiva 85/374/C sobre responsabilidad derivada de productos defectuosos y la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos COM (2022), La controversia más importante hasta ahora con respecto a este tema es la imputabilidad o la determinación del sujeto responsable, es decir, quién asume la responsabilidad de los daños que pueda causar un sistema IA. Debido a esto, y a ciertas características de autonomía, dinamicidad, capacidad de autoaprendizaje y adaptación al entorno que las configuran como tecnologías imprevisibles que escapan del control humano será preciso determinar en caso de daño quién es responsable jurídicamente.

Es “*producto defectuoso*” aquél que no ofrezca la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razonablemente previsible del mismo y el momento de su puesta en circulación. La problemática derivada de aplicar esta normativa a los efectos de la responsabilidad civil por daños causados por sistemas IA es la complejidad de la cadena de suministro: el fabricante no sería responsable si lograra probar que, en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto. Se propone a la Comisión en el Informe de 2020 sobre un régimen de responsabilidad civil en materia de IA que “*evalúe si la Directiva sobre responsabilidad por los daños causados por productos defectuosos debe transformarse en un reglamento, a que aclare la definición de «productos», determinando para ello si el contenido digital y los servicios digitales entran dentro de su ámbito de aplicación, y a que considere la posibilidad de adaptar conceptos como «daño», «defecto» y «productor»; opina que, en aras de la seguridad jurídica en toda la Unión, tras la revisión de la Directiva, el concepto de «productor» debe incluir a fabricantes, desarrolladores, programadores, proveedores de servicios y operadores finales*”: el problema sigue existiendo cuando quien haya cometido el error o fallo causante del daño no sea el fabricante, el proveedor del servicio, el diseñador, u otros intervinientes de la cadena sino un tercero o incluso el propio usuario, profesional (el médico digital) o no profesional (el usuario-paciente), de estas máquinas y sistemas.

fundamentales de los pacientes (intimidad, confidencialidad, protección de la salud psíquica, etc.) plantea el uso de aplicaciones de IA, especialmente en lo que se refiere a la interacción entre persona y robot¹¹³.

No se ha alcanzado a la fecha consenso normativo, ni tampoco doctrinal¹¹⁴, sobre este tema, muy complejo y en el que convergen intereses de difícil conciliación. Deberían, a nuestro juicio, implementarse procesos de verificación y validación preventiva en la fase previa a la comercialización de estos productos y sistemas de IA que permitan evaluar su rendimiento al exponerse a diferentes grupos por razón de edad, sexo, etnia, etc. durante ciertos periodos de tiempo¹¹⁵. Siguiendo en este punto a DE MIGUEL, debe considerarse la transparencia como un concepto dinámico¹¹⁶, y tenerse así en cuenta tanto el destinatario de la misma¹¹⁷; los objetivos que se persiguen con la transparencia¹¹⁸ y el marco o entorno institucional en el que se exige. En el caso de los productos sanitarios, ello exige distinguir entre la transparencia interna en una doble vía (hacia un proveedor de IA y hacia los proveedores de asistencia sanitaria) y la transparencia externa (hacia el paciente).

La transparencia es también un requisito fundamental en el régimen jurídico regulador de los datos personales, más aun si se tiene en cuenta que los de salud son datos personales considerados especialmente sensibles. Por ello el RGPD establece la obligación de proporcionar información “significativa” (que pueda entenderse, inteligible), que como hemos dicho encuentra su trasunto en sede de IA en el concepto de “explicabilidad”. El deber de información del art. 22.1 RGPD contempla el derecho del paciente a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles cuando puede afectar significativamente a la persona. Lo cual encuentra excepción si semejante tratamiento se basa en el consentimiento explícito del interesado, en cuyo caso y conforme al art. 22.3, tendrá el paciente derecho a expresar su punto de vista y a impugnar la deci-

¹¹³ Ebers refiere sentimientos de pudor y vergüenza, privación de la intimidad personal, problemas de dependencia o generación de adicción a las máquinas, retraimiento social y deshumanización.

¹¹⁴ Vid. DE MIGUEL ASENSIO, P. A., “Propuesta de Reglamento sobre Inteligencia Artificial”, *La Ley Unión Europea*, núm. 92, mayo 2021. LLEDÓ YAGUE, F., *Los nuevos esclavos digitales del siglo XXI y la superación del hombre óptimo ¿Hacia un nuevo derecho robótico?*, Dykinson, 2022.

¹¹⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120503/RHC_regulation_of_AI_as_a_Medical_Device_report.pdf

¹¹⁶ EBERS, M. “Transparenz und Erklärbarkeit”, en EBERS, M. (ed.), *Legal Tech Stichwort kommentar, Recht - Geschäftsmodelle-Technik*, Nomos, Baden-Baden, 2023, pp. 1239, 9 y ss.

¹¹⁷ “No es lo mismo que lo sea el usuario afectado por la decisión, un usuario experto, un científico o desarrollador de datos, un directivo, los medios de comunicación, los organismos reguladores o los tribunales de justicia...”.

¹¹⁸ Protección de derechos de las personas seguridad, fiabilidad, confianza...

sión frente al responsable del tratamiento. Por lo que es una obligación a su cargo demostrar (responsabilidad proactiva) que el paciente entiende perfectamente lo que consiente y su decisión es completamente informada¹¹⁹. El C. 60 RGPD se refiere a la obligación de informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración, obligación de transparencia a la que se hace referencia el informe “Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679” del Grupo de trabajo sobre protección de datos del artículo 29 de 3 de octubre de 2017¹²⁰.

Y en sede de los derechos y deberes dimanantes de la relación médico-paciente, tiene este último, según se infiere de lo dispuesto en el art. 42 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBRAP) derecho a ser informado también de la lógica decisional empleada por el sistema de IA, ello “de forma comprensible y adecuada a sus necesidades”: sólo mediante el reconocimiento de tal este derecho y correlativa obligación podría impugnar una decisión basada únicamente en procedimientos automatizados a la que hubiera prestado su consentimiento informado (art. 22.3 RGPD). Si esto es así, no lo es menos que en la práctica puede que la información no se halle disponible en casos de opacidad algorítmica ni aun para los mismos desarrolladores, menos aún para los responsables del despliegue. En estos casos de opacidad o “sistemas de caja negra”, los que los algoritmos son inexplicables aun por tanto para los propios expertos. Se plantea así un dilema de difícil solución: el reconocimiento de un derecho absoluto a la explicabilidad algorítmica¹²¹ podría frenar los avances científicos en la medida en que avanzamos hacia sistemas cada vez más complejos, también y por ello más eficientes, a la vez que opacos. Es por ello por lo que en esta materia ha optado el RGPD por recoger la explicabilidad en el C. 71 sin consagrarlo normativamente de forma expresa en el articulado. Los arts. 13 y 14 RGPD se refieren en caso de decisiones automatizadas y perfilados a la necesidad de proporcionar “información significativa sobre la lógica aplicada”: es decir, sobre el proceso general (de ahí que se hable de “lógica aplicada”, esto es: “ex ante”), pero no sobre el concreto proceso decisorio que ha conducido a la obtención como resultado de un determinado “output” o información de

¹¹⁹ GIL MEMBRADO, C. ob.cit, p. 151.

¹²⁰ <https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf>

¹²¹ La exigencia de explicabilidad se enfrente a un dilema, pues si bien es claramente generadora de la necesaria confianza de los destinatarios de la IA (explicación y posibilidad de impugnación de decisiones van de la mano en el ámbito jurídico que consideramos), la realidad fáctica cuando se trata de sistemas de IA demuestra, y así atestiguan los expertos, que no siempre resulta posible explicar por qué un determinado modelo ha tomado una concreta decisión y no otra diferente.

salida, que es propiamente lo que constituye la “lógica decisional”, “ex post” en la que se basa la explicabilidad. Pone la autora como ejemplo el análisis de una prueba de imagen de un paciente realizada por un sistema de IA¹²² (*recitius*: por un médico con auxilio de una IA). Si el sistema es opaco, no podrá el paciente conocer la lógica decisional que arroja como resultado un determinado diagnóstico (y no otro), para poder analizar si el proceso decisorio ha sido o no adecuado y llegado el caso, fundamentar una demanda de responsabilidad civil que permita realizar un juicio de imputación objetiva al profesional médico que ha utilizado la IA.

Lo que está claro es que los pacientes deben saber cómo y cuándo interactúan con un profesional humano y cuándo no, siendo libres de optar por alternativas de nivel equivalente: sólo de este modo, entiendo, podrá hablarse de un consentimiento suficientemente informado en el ámbito de la salud digital. En cualquier caso, entendemos que debe encontrarse un punto de equilibrio o ponderación de intereses, del mismo modo que, en el ámbito de la información sanitaria, un exceso de información podría “de facto” convertirse en desinformación por sobrecarga informativa.

2.4. APLICACIONES DE IA EN SALUD PARA USO PARTICULAR O DOMÉSTICO

Diferentes, en cuanto que no se consideran a nivel normativo sistemas de alto riesgo, son las aplicaciones tecnológicas para uso particular o doméstico¹²³ dirigidas a obtener información u orientación relativa a la salud¹²⁴: en ningún caso pueden emitir un diagnóstico, asimilándose en cierta medida a la búsqueda en bases de datos de información actualizada acerca de una enfermedad, trastorno o dolencia que aqueja al usuario. Desde luego, el RIA exige que este carácter informativo de la aplicación resulte absolutamente claro en la información de la publicidad, oferta e instrucciones de uso de estos dispositivos.

Esta IA “de riesgo limitado”, categoría que abarcaría los “chatbots” o robots conversacionales genéricos y los sistemas que permiten generar o manipular imágenes, archivos de audio o vídeos que se asemejen a perso-

¹²² En la actualidad, entre otras aplicaciones para el diagnóstico de imágenes médicas, se utiliza la IA en radiografías, tomografías computarizadas (TC), resonancias magnéticas (RM), mamografías y ecografías.

¹²³ El núm. 4 del art. 3 considera «Usuario» a toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

¹²⁴ LUQUIN BERGARECHE, R. “Aplicaciones y dispositivos de evaluación de síntomas en salud digital: aproximación jurídica”, en GIL MEMBRADO, C. y LUQUIN BERGARECHE, R. (Dir.) *Salud digital. aplicaciones móviles, telemedicina y chatbots*, Dykinson, 2024.

nas, lugares o sucesos, se rige por el principio de transparencia que obliga a advertir al usuario de su interacción con una máquina. El art. 50 RIA establece que los proveedores garantizarán que los sistemas de IA destinados a interactuar *directamente* con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate “*estén informadas de que están interactuando con un sistema de IA*” *si bien se exceptúa el supuesto* (altamente indeterminado) de que *resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización*”. El núm. dos del precepto acoge la que es una redacción de compromiso entre dos exigencias: una de orden jurídico, relativa a la necesidad de los sistemas IA de cumplir estándares elevados de eficiencia, interoperabilidad, solidez y fiabilidad y otra de orden técnico-económico, que modula el logro de dicho objetivo en la medida de los costes (elevadísimos) inherentes a su implementación y las limitaciones derivadas el estado actual de la técnica. Así, se dispone que “*Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes*”.

En este apartado de los deberes de transparencia encontramos aspectos claramente mejorables. Se establecen, como vemos, obligaciones de transparencia e información de los proveedores para con los que se denominan “responsables del despliegue” de sistemas de IA: usuarios profesionales como los médicos digitales. Sin embargo, no se imponen tales deberes a cargo de los proveedores de IA para con los usuarios-pacientes, destinatarios finales de estos servicios, u otras personas que, sin ser pacientes, hacen uso de estos productos o servicios tecnológicos complejos. Ni los proveedores ni los usuarios profesionales están obligados por el RIA a garantizar tales niveles de transparencia a las personas físicas que puedan verse afectadas por predicciones o cualesquiera decisiones o actuaciones médicas basadas o auxiliadas por sistemas y aplicaciones de IA¹²⁵: se regula el deber de informar a la persona que la aplicación con la que está interactuando es un sistema de IA “*excepto cuando resulte evidente desde el punto de vista de una persona física normalmente informada y razonablemente atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Al aplicar esta obligación, deben tenerse en cuenta las características de las*

¹²⁵ Si bien las personas afectadas deben tener derecho a obtener una explicación cuando la decisión de un responsable del despliegue se base principalmente en los resultados de determinados sistemas de alto riesgo (...) y cuando dicha decisión produzca efectos jurídicos o afecte significativamente de modo similar a dichas personas, de manera que consideren que tiene un efecto negativo en su salud, su seguridad o sus derechos fundamentales. Dicha explicación debe ser clara y significativa y servir de base para que las personas afectadas puedan ejercer sus derechos (C. 171 RIA).

*personas pertenecientes a grupos vulnerables debido a su edad o discapacidad en la medida en que el sistema de IA esté destinado a interactuar también con estos grupos*¹²⁶.

La norma en este punto es criticable por su (deliberada) ambigüedad¹²⁷: sería deseable que futuros desarrollos y actualizaciones establecieran una regulación más precisa, clara y detallada, en el sentido señalado por expertos en sus propuestas¹²⁸. De un lado, el art. 14 RIA no especifica cuándo ni cómo debe cumplirse la exigencia de la supervisión humana de la IA (“human oversight”), la cual debería extenderse a todo el ciclo de vida de estos productos, asegurando niveles adecuados de transparencia mediante la regulación de medidas concretas que no se han contemplado en el reglamento aprobado. Del mismo modo, llama la atención el silencio de una norma de este calado en lo que respecta a la implementación de guías e índices que permitan evaluar principios de justicia, igualdad y no discriminación en lo que se refiere a la IA, salvaguardando los derechos humanos y las libertades individuales de las personas en la sociedad civil.

En concreto, para usuarios finales que hacen uso v.gr de dispositivos de preevaluación de síntomas (SCA) como servicios ofertados y prestados por plataformas de gran tamaño, (reguladas en la DSA), no sólo debe ser *fiable* el sistema y la información suministrada, lo cual es esencial, sino también *inteligible*. Es decir, que su formulación permita a la persona, de modo fácilmente comprensible, conocer: i) que está interactuando con una máquina (no con un profesional médico o sanitario) y ii) que dicho sistema, máquina o robot que es la IA es incapaz ética y normativamente de adoptar con validez decisiones médicas diagnósticas o de otro tipo sin supervisión humana (“principio de autonomía supervisada de los robots”). Esta información deberá proporcionarse de forma veraz, clara, sencilla y precisa, de modo que cualquier persona destinataria (incluso personas con pocas competencias digitales) sea capaz de comprender la naturaleza y funcionalidad de estas aplicaciones. De forma tan sencilla y rápida, cuando menos, como el acceso a su utilización: a golpe de *click* y en algunos casos sin exigencia de contra-prestación inmediata.

En nuestra opinión, la regulación contenida en el RIA es cuestionable desde la perspectiva de la clasificación del riesgo cuando se trata de servicios

¹²⁶ *vid* C.132 RIA.

¹²⁷ MADIEGA, A, “Artificial Intelligence Act, Briefing”, 2 de septiembre de 2024. Disponible en [https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI\(2021\)69879](https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)69879)

¹²⁸ EBERS M, HOCH VRS, ROSENKRANZ F, RUSCHEMEIER H, STEINRÖTTER B. The European Commission’s Proposal for an Artificial Intelligence Act-A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J.* 2021; 4(4):589-603. <https://doi.org/10.3390/j4040043>

y aplicaciones de salud¹²⁹. Como resulta criticable la exclusión del ámbito de aplicación de la norma de un marco de derechos y deberes de los destinatarios finales de sistemas de IA para usos domésticos o no profesionales, usuarios de estos dispositivos para uso particular. Tampoco parece que el RIA proteja adecuadamente los intereses de los responsables del despliegue de los sistemas de IA en el ámbito médico ni los de los pacientes o usuarios finales: la previsión normativa de que los proveedores de sistemas de IA que no sean de alto riesgo se sujeten a códigos de conducta voluntarios resulta claramente insuficiente desde el punto de vista de la salvaguarda de derechos, habida cuenta de la posibilidad de eludir la aplicación del RPS evitando el fabricante calificar su finalidad como sanitaria (y con ello, la consideración de sistema de alto riesgo de un dispositivo de IA), en un campo en el que los riesgos pueden materializarse en daños que afectan a la vida, salud y derechos fundamentales de las personas.

2.5. EL RIA COMO SISTEMA NORMATIVO DE PREVENCIÓN DEL RIESGO: REMISIÓN A OTROS MARCOS REGULATORIOS EN EL ÁMBITO DE LOS DAÑOS CAUSADOS POR SISTEMAS DE IA EN SALUD

La coexistencia de otros conjuntos normativos específicos en la UE íntimamente relacionados con la regulación de la IA en el campo de la salud (protección de datos personales, productos sanitarios, productos defectuosos, responsabilidad civil extracontractual) complica aún más un terreno regulatorio complejo y delicado. Como se ha visto, la IA en el ámbito de la salud se halla íntimamente relacionada con los productos sanitarios y los componentes de los mismos. El RIA configura por ello un “ecosistema normativo” incompleto en cuanto debe complementarse con otros subsistemas regulatorios, entre ellos:

- i. El marco jurídico de protección de datos personales¹³⁰: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de es-

¹²⁹ El título III RIA contiene normas específicas para aquellos sistemas de IA que acarrearán un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas, permitidos la Unión si cumplen determinados requisitos obligatorios y se someten a una evaluación de la conformidad *ex ante*. Ahora bien: la clasificación de un sistema de IA como de alto riesgo no depende únicamente de la función que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se use dicho sistema, lo que introduce elementos de complejidad y duda en algunos supuestos.

¹³⁰ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

tos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos ha sido modificado parcialmente por el Reglamento (UE) 2023/2854 de 13 de diciembre de 2023);

- ii. El marco regulatorio de los productos sanitarios, contenido en el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios¹³¹ y, en nuestro ordenamiento, en el Real Decreto 192/2023, de 21 de marzo¹³²;
- iii. El marco regulatorio cuando el sistema de IA puede calificarse como “producto defectuoso” productos defectuosos: debe tenerse en cuenta la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, que aprueba la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos¹³³;
- iv. En lo que se refiere a responsabilidad extracontractual por daños causados por IA, la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA) de 28 de septiembre de 2022¹³⁴.

Además no hay que olvidarse que, cuando es el usuario no profesional el que hace uso de aplicaciones de IA en el contexto de contratos de servi-

¹³¹ Un robot o sistema de IA puede tener la consideración (o no) de producto sanitario de conformidad con el RPS entendido como “todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación”. Debe para ello ser utilizado con finalidad médica específica de “diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad; diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad; investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico; obtención de información mediante el examen “in vitro” de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos, y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos”.

¹³² Los productos sólo pueden introducirse en el mercado, comercializarse y/o ponerse en servicio si cumplen los requisitos establecidos en el Reglamento (UE) 2017/745 cuando hayan sido debidamente suministrados, estén correctamente instalados y mantenidos siguiendo las indicaciones del fabricante, y se utilicen conforme a su finalidad prevista, no comprometiéndola la seguridad ni la salud de los pacientes, de los usuarios ni, en su caso, de terceros (núm. 1). Sólo podrán utilizarse en España productos que cumplan las disposiciones del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, en las condiciones y según las finalidades previstas por el fabricante de los mismos (art. 5).

¹³³ https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.html

¹³⁴ <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496>

cios de telemedicina (por adhesión con condiciones generales) contratados con grandes proveedores de este tipo de servicios, ostenta la condición de “consumidor”, por lo que le será aplicable el régimen de protección previsto en el TRLGDCU, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre¹³⁵. En el ámbito de la Unión Europea, debe tenerse en cuenta el marco regulador de la prestación de servicios digitales previsto en la reciente Directiva de Mercados Digitales (DMA) y en la Directiva de Servicios Digitales (DSA)¹³⁶. En lo que se refiere a los contratos de suministro de contenidos y servicios digitales, deberá tenerse en cuenta lo dispuesto en el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales)¹³⁷.

Así, el marco regulatorio del RIA tiene un carácter horizontal y excesivamente amplio y no introduce orden entre estos conjuntos normativos tan diversos cuando se trata de daños causados por sistemas de IA¹³⁸: las distintas normas parten incluso de definiciones diversas de los agentes involucrados e incluso de las categorías de riesgo¹³⁹. Si bien se establecen obligaciones de transparencia e información de los proveedores para con los usuarios profesionales “responsables del despliegue” de estos sistemas, hay que lamentar que en el RIA no se hayan regulado deberes a cargo de aquéllos para con los usuarios-pacientes y otras personas que hacen uso de estos productos o servicios tecnológicos complejos (v.gr, ancianos o personas dependientes en residencias geriátricas o en entornos no clínicos).

¹³⁵ El art. 93 TRLGDCU excluye del ámbito de aplicación de las normas sobre este particular a “los contratos de servicios relacionados con la salud, prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios, con independencia de que estos servicios se presten en instalaciones sanitarias”: exclusión debida a que la asistencia sanitaria exige una regulación especial debido a su complejidad técnica, su importancia como servicio de interés general y su financiación pública.

¹³⁶ <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0825&from=en>

¹³⁷ En la DSA se definen las responsabilidades a cargo de los prestadores de servicios intermediarios, especialmente las plataformas en línea como los mercados y las redes sociales, determinando la imposición de obligaciones de “diligencia debida” (concepto jurídico indeterminado no exento de problemas a la hora de su concreción práctica) para determinados intermediarios, incluyendo procedimientos de notificación y acción en relación con los contenidos ilícitos y la posibilidad de impugnar las decisiones de moderación de contenidos de las plataformas.

¹³⁸ En caso de contradicción, ¿prevalece el RIA como normativa de detalle o el RPS como “*lex specialis*”?

¹³⁹ Mientras aquella califica todos los productos sanitarios en el sentido del RPS como de “alto riesgo”, el RPS establece, de forma más matizada, una tipología que va desde el *bajo riesgo* (clase I), el *riesgo medio* (clases IIa y IIb) el *alto riesgo* (clase III), de modo que un sistema de IA podría calificarse de *alto riesgo* con arreglo a la propuesta de la LIA, y RPS lo haga como de *riesgo medio*.

Ni los proveedores ni los responsables del despliegue de los sistemas están obligados a garantizar información transparente a la persona física que, como destinatario final, resulte afectada por una predicción o decisión basada en IA, lo cual origina una situación de indefensión explicable desde criterios de eficiencia pero difícilmente justificable desde principios jurídicos y éticos.

2.6. FORMACIÓN Y CAPACITACIÓN EN IA DEL PROFESIONAL DE LA SALUD

Finalmente debemos hacer referencia a la necesidad de que los médicos y profesionales de la salud en general refuercen sus conocimientos, competencias y habilidades en lo que se refiere a estas tecnologías que indudablemente representan un avance para la medicina y los pacientes. El desafío (en última instancia, económico y normativo) al que se enfrentan en este punto administraciones públicas y entidades privadas en el momento crítico en que nos encontramos es enorme.

El RIA se refiere a un resultado que no puede vislumbrarse como lejano en Europa. Urge adaptarnos, y con rapidez, a estos avances. En este punto, el art. 4 LIA regula lo que se denomina “alfabetización en materia de IA”¹⁴⁰, estableciendo que los proveedores y responsables del despliegue de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas. De nuevo, el empleo de conceptos jurídicos altamente indeterminados (“en la mayor medida posible”, “nivel suficiente”...) es muestra de la prisa del legislador comunitario por alcanzar una norma de consenso que permita disponer cuanto antes de un marco regulatorio aplicable a una realidad fáctica altamente compleja en vertiginoso desarrollo.

¹⁴⁰ Según el C. 56, la «alfabetización en materia de IA» comprende las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del RRI, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

3. DAÑOS CAUSADOS EN INTERVENCIONES MEDICAS CON AUXILIO DE IA: REDEFINICION DE LA “LEX ARTIS” Y FUNDAMENTOS DE LA RESPONSABILIDAD

3.1. CUANDO EL MÉDICO SE PREVALE DE UN SISTEMA DE IA Y SU ACTUACIÓN CAUSA DAÑOS: PRESUPUESTOS DE LA OBLIGACIÓN DE RESPONDER

La IA va a tener cada vez más relevancia como elemento auxiliar del profesional médico en la toma de decisiones, y ello incluye su actividad diagnóstica, pronóstica, terapéutica, quirúrgica y rehabilitadora.

En la función de diagnóstico, estos sistemas ofrecen al profesional la posibilidad de un acceso rápido a información clínica o relativa a investigaciones científicas, lo cual se manifiesta especialmente en el campo del análisis de imágenes clínicas. En esta especialidad médica se está utilizando ampliamente la IA en tomografías computarizadas, rayos X, resonancias magnéticas y otras imágenes en busca de lesiones, tumores, etc. que un radiólogo humano podría pasar desapercibidos. La IA impulsada por redes neuronales artificiales (la más compleja y autónoma, basada en redes neuronales profundas) optimiza la fiabilidad de la decisión diagnóstica, facilita el procesamiento de la ingente cantidad de información exigible y personaliza la atención, focalizándola sobre el paciente y su singular historia clínica.

Dispositivos de IA permiten en las UCI la observación y seguimiento de los signos vitales de pacientes receptores de cuidados intensivos, alertando a los médicos del incremento de factores de riesgo. Debido a que los modelos de IA pueden aprender (“machine learning”), la IA tiene el potencial de proporcionar recomendaciones personalizadas en tiempo real a los pacientes, incrementando las ventajas de una atención personalizada a la vez que reduciendo los costes económicos, temporales y emocionales para todos los implicados.

En cirugías, entre otras aplicaciones, los nuevos sistemas de laparoscopia y para implantes de cóclea mejoran la precisión del médico y en intervenciones quirúrgicas de complejidad, la precisión, seguridad y mínima invasión de los robots quirúrgicos (v.gr sistemas dotados de sensores de IA para la realización de cateterismos cardiacos) redundan en la obtención de mejores resultados para los pacientes¹⁴¹.

¹⁴¹ Vid. <https://www.intuitive.com/en-us/products-and-services/da-vinci>

También se utilizan hoy aplicaciones de IA y robots en la rehabilitación de enfermedades y lesiones: entre muchas otras aplicaciones médicas y de fisioterapia, en el tratamiento posterior a accidentes de circulación mediante ejercicios físicos, o enfermedades cerebro-vasculares.

En el campo de la salud mental, los “chabots” y robots actúan ya (en algunos casos y para ciertos perfiles de pacientes y patologías, trastornos y enfermedades mentales) como ayuda de los psicoterapeutas virtuales y pueden ayudar en el tratamiento de problemas psicológicos como la ansiedad o la depresión (Ebers¹⁴²), ofreciendo herramientas para trabajar sus síntomas o desarrollar habilidades sociales. También la IA puede desempeñar una función de apoyo a ancianos y personas dependientes que puede resultar cada vez más relevante en sociedades de envejecimiento poblacional exponencial.

Se hace necesario distinguir en este ecosistema de prestación de servicios de salud digital diversas relaciones jurídicas: a. La que liga al fabricante o diseñador de un sistema de IA que normativamente puede considerarse producto defectuoso frente al consumidor o usuario que sufre un daño como consecuencia del mismo; y b. La existente entre el centro hospitalario que pone a disposición de sus profesionales sistemas de IA para que les auxilien en el desempeño de sus funciones el centro médico u hospitalario y el paciente que sufre el daño.

Nos centraremos en este trabajo en la responsabilidad civil derivada de servicios médicos, entendiendo por tales los prestados por profesionales en el ejercicio de sus funciones diagnósticas, terapéuticas, quirúrgicas y rehabilitadoras con auxilio de sistemas de IA, intentando dar respuesta al interrogante formulado al comienzo del trabajo: si debe el médico responder, y en caso afirmativo, en qué casos y bajo qué fundamentos, de los daños causados en su actividad diagnóstica o pronóstica, terapéutica, quirúrgica o rehabilitadora cuando se apoya o auxilia en robots o sistemas de IA. Si bien tomamos como punto de partida la relación jurídico-privada de prestación de servicios médicos, la mayor parte del análisis puede trasladarse a los supuestos de daños originados en el ámbito de un hospital o centro sanitario público en que, como es sabido, es de aplicación el régimen (de responsabilidad objetiva) previsto en la Sección 2ª del Cap. IV de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público¹⁴³.

¹⁴² “The Top 12 Healthcare Chatbots”, Medical Futurist, 2021. <https://medicalfuturist.com/top-12-health-chatbots/> citado por EBERS, M. ¿Terapia sin terapeutas?, en LUQUIN BERGARECHE, R (Dir.) *Servicios privados de telemedicina y Salud Digital: retos e implicaciones jurídicas*, Tirant lo Blanch, 2023, pp.32 y siguientes.

¹⁴³ En la Sección 1ª, el art. 32 (“Principios de la responsabilidad”) dispone en su núm. 1 que “Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, siempre que la lesión sea

Tampoco se abordará en este trabajo el actual régimen jurídico de responsabilidad de IA que sea producto defectuoso, cuestión íntimamente relacionada con el tema que nos ocupa, pero sujeto a una normativa específica.

Con carácter general, la prosperabilidad de la acción para exigir el resarcimiento de un daño causado por un profesional que presta un servicio, como el médico (nos referiremos en particular a la contractual, sin perjuicio del reconocimiento jurisprudencial del principio de unidad de la culpa civil¹⁴⁴) requiere a tenor de la jurisprudencia, acreditar cumplidamente los siguientes elementos:

- a) La existencia de una relación jurídica contractual entre las partes: la relación que vincula al médico con el paciente es un arrendamiento de servicios¹⁴⁵;

consecuencia del funcionamiento normal o anormal de los servicios públicos salvo en los casos de fuerza mayor o de daños que el particular tenga el deber jurídico de soportar de acuerdo con la Ley”.

El art. 36, que lleva por título “Exigencia de la responsabilidad patrimonial de las autoridades personal al servicio de las Administraciones Públicas” establece que:

“1. Para hacer efectiva la responsabilidad patrimonial a que se refiere esta Ley, los particulares exigirán directamente a la Administración Pública correspondiente las indemnizaciones por los daños y perjuicios causados por las autoridades y personal a su servicio.

2. La Administración correspondiente, cuando hubiere indemnizado a los lesionados, exigirá de oficio en vía administrativa de sus autoridades y demás personal a su servicio la responsabilidad en que hubieran incurrido por dolo, o culpa o negligencia graves, previa instrucción del correspondiente procedimiento.

Para la exigencia de dicha responsabilidad y, en su caso, para su cuantificación, se ponderarán, entre otros, los siguientes criterios: el resultado dañoso producido, el grado de culpabilidad, la responsabilidad profesional del personal al servicio de las Administraciones públicas y su relación con la producción del resultado dañoso”.

¹⁴⁴ Debe tenerse en cuenta cuando abordamos la responsabilidad sanitaria la aplicación del principio de “unidad de la culpa civil” reconocido jurisprudencialmente (entre otras, STS 627/2006, 8 de Junio de 2006...) conforme al cual en supuestos donde concurren acciones basadas en un incumplimiento contractual y en un ilícito extracontractual, se ofrece al perjudicado (en beneficio de la indemnizabilidad del daño) la facultad de optar por ejercitar la acción cuya naturaleza estime más conveniente o ambas acciones de forma conjunta, formulando en la demanda una solicitud alternativa o incluso acumulada. Incluso se admite que el perjudicado aporte al juzgador que se presume conoce el derecho (“iura novit curia”) tan sólo los hechos en los que basa su reclamación para que sea aquél quien decida sobre el tipo de responsabilidad a su juicio procedente (“da mihi factum, dabo tibi ius”) y determine la naturaleza de la acción y consiguiente fundamentación normativa, con efectos de tanta trascendencia como el diferente plazo de prescripción de la acción ejercitada.

¹⁴⁵ “En el arrendamiento de obras o servicios, una de las partes se obliga a ejecutar una obra o a prestar a la otra un servicio por precio cierto” (art. 1544 CC).”.

El art. 586 de la Propuesta de Código Civil de la APDC establece la siguiente regulación del contrato de servicios médicos:

“1. Por el contrato de servicios médicos el médico, o el centro, servicio o establecimiento sanitario se obliga frente al paciente a realizar el acto o el tratamiento conforme a lo previsto en el contrato y los estándares de la medicina exigibles, a cambio de la remuneración pactada.

2. Las disposiciones del presente Capítulo son de aplicación cuando la prestación de los servicios médicos constituye el contenido de un contrato de seguro de asistencia médica (...).”.

A la prestación del servicio médico digital de conformidad con autonomía negocial y los “estándares de la medicina exigibles”, debería quizá añadirse la adecuación, también, a “las normas jurídicas y los estándares éticos de las nuevas tecnologías y de la Inteligencia Artificial”.

- b) Que se hayan incumplido total o parcialmente una o varias obligaciones derivadas de ese vínculo negocial. Como es sabido, la obligación principal del médico es de medios, no de resultado, salvo en medicina satisfactiva: intentar la “cura” del paciente, entendida como el mantenimiento y recuperación de su salud manteniendo los estándares exigibles, de conformidad con los protocolos y las guías de actuación médica. Pero también, tras la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, se incluye en la “lex artis” del médico la de información asistencial (art. 4) acerca de la naturaleza, consecuencias y riesgos de intervención que permita al paciente prestar un consentimiento informado válido (art. 8). Sólo de este modo podrá hablarse de la “autonomía del paciente”, que se torna en autorresponsabilidad (responsabilidad proactiva) en el nuevo contexto de la salud digital. Aunque no se halle previsto en una norma que ha quedado obsoleta, como veremos debe entenderse comprendida a estos efectos la información del médico al que se ha venido a llamar “paciente digital” acerca de los riesgos inherentes a estas aplicaciones tecnológicas, a fin de posibilitar optar por otros cursos de acción alternativos (no es otro el fundamento e interés jurídico protegido por tal derecho a la autodeterminación del paciente en el ámbito de su salud);
- c) Que el incumplimiento, total, parcial o defectuoso, de la prestación a la que se obliga el médico sea culposo¹⁴⁶: esto es, negligente, falta de prudencia, de cuidado, el que es exigible en el ejercicio de su profesión (“lex artis”) en un caso concreto y habida cuenta de sus circunstancias (“ad hoc”). La culpa implica un actuar carente de la diligencia exigible en cada supuesto en atención a las circunstancias de las personas, del tiempo y del lugar: el profesional a quien se imputan los daños está obligado a acreditar, para ser exonerado de responsabilidad, su actuar diligente (cuando se trata de culpa extracontractual, la carga de la prueba corresponde al perjudicado, si bien la jurisprudencia consagra una inversión del “onus probandi” o carga de la prueba de la culpa por la mayor accesibilidad de los profesionales médicos a las historias clínicas y otros medios de prueba. De modo que no debe el paciente perjudicado probar la culpa sino excepcionar el médico demandado acreditando que el daño causado no fue debido a su actuar negligente (salvo en los supuestos en

¹⁴⁶ La culpa contractual consiste en la acción u omisión voluntaria, pero realizada sin malicia, que impide el cumplimiento normal de una obligación (Castán).

que sea aplicable la doctrina del daño desproporcionado o de la “res ipsa loquitur”), entre otros expedientes de facilitación de la prueba reconocidos juriprudencialmente¹⁴⁷;

- d) Existencia de un nexo o relación de causalidad (causa-efecto entre el hecho y el resultado, físico y jurídico). Al que alega un hecho, le corresponde en derecho probarlo y esta prueba puede no ser fácil en casos en que intervienen múltiples agentes diferentes en el acto médico o si el médico se auxilia con un sistema de IA. Por el denominado principio de “unidad de la culpa civil”¹⁴⁸, tanto en la responsabilidad contractual como en la extracontractual, la causalidad se perfila a través de la denominada “causalidad adecuada” y “eficiente”, conforme a la cual se traslada la trascendencia de la prueba al “*nexo causal*”;
- e) Imputabilidad del agente, juicio de imputación o causalidad jurídica, que implica que el resultado pueda jurídicamente imputarse al agente de acuerdo los anteriores criterios;
- f) Relacionado con el punto anterior, para que se desencadene el efecto resarcitorio-indemnizatorio es preciso que no concurra la intervención de una fuerza externa totalmente imprevisible o bien previsible pero inevitable (caso fortuito o fuerza mayor): piénsese, por ejemplo, en una interrupción en el suministro de energía eléctrica no subsanable por otros medios) o intervención de terceros que rompan el nexo de causalidad (v.gr. ciberdelincuencia). Tampoco el

¹⁴⁷ Si bien este trabajo se circunscribe a los servicios médicos que se prestan en el ámbito privado, deberá hacerse referencia a las particularidades de régimen jurídico previsto para los daños causados por médicos que actúan al servicio de administraciones públicas en centros u hospitales de esta naturaleza. La responsabilidad en este caso es objetiva a tenor de lo dispuesto en la LRJSP que hace responsables a las administraciones públicas por el funcionamiento normal o anormal de los servicios públicos: la exención de la obligación de prueba de la culpa en estos casos no implica la de la relación de causalidad, y la acreditación del daño y su cuantificación.

¹⁴⁸ Entre otras, SSTS 550/2008, de 18 de junio; 537/2013, de 14 de enero y 661/2017. La STS (Sala 1ª) de 12 de diciembre de 2017 dispone que “la jurisprudencia de esta Sala admite la posibilidad de un cambio en la calificación jurídica de los hechos en los supuestos de error o imprecisión de la parte, si bien este cambio debe extraerse de los propios hechos alegados y conformados, en cuanto han podido ser objeto de discusión sin alterar los términos del debate siempre que no haya podido causar indefensión a cualquiera de los litigantes. Ocurre que la parte actora a la hora de fijar estos hechos no establece como controvertida si la relación era contractual o extracontractual ni desvirtúa la relación extracontractual que siempre mantuvo la demandada, en razón a la relación jurídica establecida entre las partes, y sobre ella resuelve la sentencia, pues los hechos seguían siendo los mismos. La sentencia, en definitiva, da respuesta a lo que se plantea en relación a la llamada unidad de culpa civil (..) para entender que la acción ejercitada en la demanda no es otra que la extracontractual y no la contractual y sus conclusiones sobre la naturaleza jurídica de la acción en función de los hechos alegados no tiene otro cauce revisorio que la del recurso de casación” (F.D. 2º).

daño debería ser imputable al perjudicado por incumplimiento de alguno de los deberes que le incumben: en su cualidad de paciente, entre otros previstos en la LBRAP, el que contrata este tipo de servicios debe proporcionar información veraz acerca de su estado de salud o enfermedad y atenerse durante su tratamiento a las instrucciones facilitadas por el facultativo, incluidas en su caso las relativas al uso adecuado de los dispositivos médicos de carácter tecnológico;

- g) Que el daño o perjuicio sea reparable y cuantificable. El art. 1106 CC dispone que “la indemnización de daños y perjuicios comprende, no sólo el valor de la pérdida que hayan sufrido, sino también el de la ganancia que haya dejado de obtener el acreedor (...)”. Es importante en este punto hacer referencia a que se incluyen como resarcibles tanto los daños materiales o económicos, en su doble modalidad de daño emergente y lucro cesante, como también los daños morales (a diferencia del régimen de productos defectuosos, en que sólo tiene encaje la indemnización de los daños patrimoniales).

Queda para un ulterior trabajo el análisis de la “lex artis” del médico digital en el nuevo escenario de salud digital y los mencionados presupuestos de la responsabilidad civil del médico que se auxilia por la IA. Con un alcance más modesto, el trabajo que recoge esta ponencia se limita a continuación a exponer algunas particularidades que presenta el régimen de responsabilidad civil de los profesionales médicos que se auxilian con robots, aplicaciones o sistemas de IA en el ejercicio de sus funciones.

3.2. CARACTERES DE LOS SISTEMAS DE IA EN SALUD: EN PARTICULAR, LA INFLUENCIA DEL GRADO DE AUTONOMÍA DEL ROBOT O SISTEMA AUXILIAR DE IA EN LA RESPONSABILIDAD POR DAÑOS

Los robots o aplicaciones de IA son sistemas complejos, interconectados y dinámicos. Además de estos caracteres, que se proyectan sobre el régimen de responsabilidad civil del profesional médico que se prevale de ellos como medio auxiliar, en este ámbito deben tenerse en cuenta variables como su grado de autonomía (o la de sus componentes), el desempeño de un rol más o menos activo en la intervención de que se trate y la fase del procedimiento en que intervengan.

No todos los robots, dispositivos o sistemas médicos de IA son iguales: debe partirse de la distinción entre sistemas o robots *autónomos*, que son aquellos que no requieren de intervención humana, actuando por sí mismos y sistemas *teleoperados*: estos últimos son los que vienen implementándose desde

hace ya algunas décadas y requieren del control del médico o cirujano a través de órdenes introducidas a una computadora o por medio de una interfaz informática controlada manualmente. Aquellos no están admitidos por el RIA conforme al principio de necesidad de supervisión de la IA, pero dentro de estos últimos, resulta relevante a efectos de la determinación de la “lex artis ad hoc” del profesional sanitario (y consiguiente responsabilidad por daños, en su caso) la tipología que clasifica a los robots médicos en atención a su rol tomando en consideración la distribución de riesgos médico-robot¹⁴⁹: desde el desempeño de un rol pasivo, en el que la intervención clínica de la “maquina” y, por ende, la posible asunción de riesgos de su fabricante, diseñador o responsable del despliegue es mínima, pasando por un robot de rol restringido -como algunos laparoscopios- en el que la responsabilidad puede ser compartida (pues el facultativo médico interviene en algunas fases del procedimiento)¹⁵⁰, hasta robots de rol activo, en los que el sistema de IA desarrolla y controla fases muy arriesgadas del procedimiento: esto es, relevantes y condicionantes del éxito o fracaso de la intervención clínica¹⁵¹.

También en atención a la interacción médico-sistema de IA, no es lo mismo en orden a valorar el grado de asunción de responsabilidad médica un sistema cuya activación precisa necesariamente la voz humana o actos como pisar un pedal o mover un joystick que otro que se ponga en funcionamiento a través de un sistema tecnológicamente más complejo, o incluso automática-

¹⁴⁹ El robot quirúrgico “Da Vinci” es un sistema rol activo con una autonomía reducida. El “Automated Endoscopic System for Optimal Positioning” (AESOP) es un robot de rol restringido pero con una autonomía plena. Controlado a través de un ordenador, su función es el posicionamiento óptimo del laparoscopio: es activo al dirigir su propio movimiento sobre la base de ciertas instrucciones de voz del cirujano y su rol es restringido porque su finalidad es la colocación del laparoscopio para asegurar una imagen nítida del interior del paciente que facilita la intervención. “Neuromate” es un robot de posicionamiento y orientación de los instrumentos quirúrgicos que serán controlados por el cirujano de forma manual: su finalidad básica es la de estabilizar y facilitar la ejecución del procedimiento quirúrgico. Su rol activo se debe a que ejerce múltiples funciones dentro de la operación, algunas de ellas de bastante invasividad. “Robodoc” es semiactivo porque el cirujano tiene una labor primordial en la primera fase (la elaboración del plan preoperativo), mientras que el robot actúa autónomamente en la segunda (ejecución del plan). El rol restringido se debe a que en los procedimientos quirúrgicos en los que se aplica el robot solamente asume una elevada carga de riesgo en una parte del procedimiento. BLOOM, SALZBERG, and KRUMMEL (2002), citado por GARCÍA MICO, T.G. “Litigación asociada a la cirugía robótica con el Da Vinci”, *Indret Revista para el Análisis del Derecho*, octubre de 2014.

¹⁵⁰ MURPHY et al. (2008, p. 1077) se refieren en función de la capacidad de acción permitida al profesional, a los grados de libertad del profesional médico (“degrees of freedom”). El llamado índice DOF mide la similitud del instrumento quirúrgico robótico o mecánico con la mano humana. A más DOF, más parecida será la cirugía a una practicada por la mano humana; y a menos, mayor dificultad va a presentar. Según BLOOM, SALZBERG & KRUMMEL (2002, p. 747). <http://www.medicaexpo.com/prod/lut/endoscopes-rigid-right-angled-laparoscopes-working-channel>

¹⁵¹ TAYLOR, R. H.; STULBERG, S. D. Medical robotics working group section report. En *Proc. NSF Workshop Medical Robotics and Computer-Assisted Medical Interventions (RCAMI)*. 1996.

mente. Distinguen los expertos¹⁵² a estos efectos entre sistemas: (i) *semiactivos*, dotados de dispositivos de interfaz como pedales, joysticks, mecanismos de activación por voz, etc., en los que hay una interacción parcial del médico o cirujano, que controla el dispositivo en determinadas fases del procedimiento mientras que en otras éste actúa sin necesidad de órdenes humanas ni guía de facultativos¹⁵³; y (ii) *pasivos*, en los que el sistema o robot es incapaz de intervenir por sí mismo, necesitando al médico para su funcionamiento y actuación en todo caso.

Si tomamos como ejemplo el conocido “Da Vinci Surgical System”, robot quirúrgico de última generación que se aplica a una multiplicidad de procedimientos médicos, principalmente en urología y la cardiología (la cirugía cardíaca per se es altamente riesgosa), su rol es muy activo pero requiere del control manual del cirujano por medio de una interfaz informática (además de la preparación, supervisión, etc.), por lo que no exime al profesional médico de la obligación de responder por el daño causado si resulta acreditado que no cumplió el cirujano debidamente las instrucciones que se le hayan facilitado observando el nivel de diligencia que exige la “lex artis ad hoc” en la ejecución de estas intervenciones.

El incumplimiento a estos efectos del deber de información del productor (fabricante, diseñador..) de la IA al “responsable del despliegue” (hospital, centro de salud, médicos) es fundamental. Su ausencia permite imputar la responsabilidad al productor por no haber puesto a disposición del proveedor del servicio de asistencia sanitaria toda la información disponible: para ello, entablada una demanda de responsabilidad civil, debería probarse en el proceso judicial que el productor no ofreció la información¹⁵⁴ que habría llevado a las partes implicadas a percatarse de los riesgos inherentes al producto¹⁵⁵. Se trata

¹⁵² Ob. cit, p. 749.

¹⁵³ Actualmente son frecuentes las cirugías no invasivas en las que el cirujano se auxilia de tecnologías innovadoras, algunas de ellas sistemas de IA, que permiten una mayor o menor autonomía o independencia al profesional médico. Los modernos laparoscopios llevan integrada una cámara de alta definición que les permite observar en tiempo real el desarrollo de la intervención y controlar los instrumentos endoscópicos manualmente. El principal hándicap es el efecto espejo que obliga a que la manipulación de los instrumentos endoscópicos deba verificarse en la dirección contraria a la pretendida.

¹⁵⁴ PASQUAU LIANO, 2013, pp. 159-178.

¹⁵⁵ La STS, 1ª, 3.12.1997 (RJ 1997/872) resolvió el caso de una máquina que causó daños a la víctima por no ser posible seleccionar la tronadora adecuada al soporte, siendo la causa la insuficiente información presentada por el importador. Para el Tribunal Supremo, esa falta de información permite deducir la causa del accidente, afirmando que “la acción efectuada por la empresa recurrente de poner en circulación un producto evidentemente peligroso sin haber cumplido con un deber de información adecuado implica responsabilidades; afirmación, ésta, absolutamente correcta, y que se infiere del dato de que el accidente se ha producido por una utilización inadecuada de la máquina en cuestión, y porque no se dijo o se puso en conocimiento de la víctima o se informó a la misma, cuáles eran las medidas de seguridad y protección para un uso correcto que normalmen-

de un tema de imputabilidad pero también de determinación del nexo de causalidad: causalidad que debe ser “adecuada” entre la omisión de un agente y la producción del resultado dañoso.

Cuando hablamos de prestación de servicios médicos con sistemas de IA, debe tenerse en cuenta que los robots o sistemas están integrados por un “hardware” (el elemento tangible, por ejemplo el smartphone o el ordenador) y un “software” (el programa informático). Por su propia naturaleza, el software presenta como riesgo inherente la vulnerabilidad resultante de su exposición a conductas de terceros como hackeos o ataques informáticos, debido a su interconexión con una red que es global. El riesgo, ciertamente, puede controlarse pero no hay “riesgo cero” en estos casos, incluso cuando el responsable del diseño haya extremado su diligencia en este punto.

Ante el interrogante de si, materializado el hackeo de un sistema de IA en salud que ha provocado un daño a un paciente, podría el perjudicado invocar un defecto de información como causa en la que fundamentar el juicio de imputabilidad al médico, entiendo que la respuesta sería afirmativa excepcionalmente si se cumplen ciertas condiciones: i. que el fabricante haya adoptado por su parte las medidas técnicas¹⁵⁶ tendentes a la evitación o minimización de este riesgo (en caso contrario, respondería de forma objetiva, lo cual será lo más frecuente); y ii. Que el médico responsable de la intervención auxiliada por un sistema de IA haya actuado diligentemente y habiendo efectuado en tal sentido al paciente una advertencia suficientemente clara e inteligible a fin de prestarse un consentimiento verdaderamente informado: su ausencia habría podido impedir la libre elección entre un curso de acción u otro (la cirugía robótica con sus indudables ventajas, la cirugía laparoscópica -de ser posible- o la clásica cirugía abierta).

3.3. RELACIÓN DE CAUSALIDAD. LA CAUSALIDAD FÍSICA Y SU PRUEBA

La causalidad material, “causalidad de hecho” o “causalidad física” es la primera de las fases en la determinación del nexo causal como presupuesto

te deben contar en un manual de instrucciones, el cual no se proporcionó. Con lo cual surge, además la causalidad suficiente, dato que suscribe absolutamente esta Sala” (FD 2°).

¹⁵⁶ Según GARCÍA MICÓ, refiriéndose al robot quirúrgico Da Vinci, sería necesario: “Primero, que el desarrollo técnico del software haya sido realizado de modo que no presente ninguna vulnerabilidad conocida conforme al estado de los conocimientos científicos y técnicos. La inobservancia de este extremo podría servir para sostener la existencia de un defecto de diseño manifiesto; segundo, que se dote al robot de la capacidad de detectar la intromisión; tercero, y último, que el software disponga de mecanismos de bloqueo de su propio funcionamiento en caso de que se detecte que un tercero ha podido superar los sistemas de seguridad y ha tomado el control del sistema”. GARCÍA MICO, TG ob. cit, p. 20.

del resarcimiento del daño y tiene como fin valorar si una determinada acción u omisión es la que ha dado lugar al concreto daño cuyo resarcimiento se solicita.

Los caracteres de la IA (complejidad, opacidad e interconectividad, fundamentalmente), dificultan averiguar qué defecto concreto ha causado un determinado daño, que incluso pudiera hacerse imposible en los sistemas de aprendizaje automático. Son muchos los agentes que intervienen en una IA dada la interconectividad y la dependencia de estos sistemas: desde el fabricante del hardware, al diseñador del software, el programador, el responsable de su despliegue o persona, física o jurídica, que se sirve del mismo pueden ser responsables¹⁵⁷, y ello debido a muy diversos factores: fallos en los algoritmos, sesgos en los datos introducidos como inputs, fallos de conectividad (conexión a la red, fallos en los dispositivos interconectados), vulnerabilidades a ataques informáticos, etc.

Una aplicación rigurosa de la teoría de la equivalencia de las condiciones o “*conditio sine qua non*” (o el “*but for test*” del derecho anglosajón de daños “*Tort Law*”: “*but for the action, the result would not have happened*”) abocaría, como afirma EVANGELIO, a la no imputación del daño a ninguno de los posibles agentes, por lo que para evitar esta consecuencia injusta, se recurre a la responsabilidad solidaria cuando resulte imposible o muy difícil la individualización de la causa concreta del daño (a modo de presunción *iuris tantum*). O según otros autores, al recurso a la regla de la responsabilidad proporcional recogida en los arts. 3:103-3:106 PETL, que distribuye la responsabilidad de manera proporcional a la probabilidad del riesgo de causación, criterio desde luego más equitativo pero de difícil implementación práctica en cuanto implica la necesidad de probar tal “mayor probabilidad”, lo cual dependerá del estándar de prueba existente en cada ordenamiento jurídico. Este estándar es más alto, como se sabe, en los de derecho continental como el español¹⁵⁸ que en los países del Common Law: en los primeros, los que jueces y tribunales pueden llegar a exigir un grado de convencimiento “más allá de toda duda razonable”, lo que implica “una probabilidad rayana en la certeza”, en tanto en los países anglosajones, es suficiente pasar el test de ser posibilidad más probable entre dos hipótesis contrapuestas: “*more probable than not*”).

¹⁵⁷ También habría que hacer alusión a la posible responsabilidad de este último, el “paciente digital”, en la producción o, más habitualmente, contribución causal a la materialización del daño cuando por su parte haya incumplido algunos de los deberes que se le imponen normativamente (v.gr, la transmisión veraz de información relativa a su enfermedad o proceso de salud).

¹⁵⁸ REGLERO CAMPOS, L.F. Y MEDINA ALCOZ, L. “El **nexo causal**. La pérdida de oportunidad. Las causas de exoneración de responsabilidad: culpa de la víctima y fuerza mayor”. REGLERO CAMPOS, L.F. (COORD.), BUSTO LAGO J.M. (coord.), *Tratado de responsabilidad civil*. Thomson Reuters Aranzadi, 2014.

3.4. LA CAUSALIDAD JURÍDICA: EL JUICIO DE IMPUTACIÓN

Una vez establecido y acreditado el nexo de causalidad física o material, habrá que determinar cuál de estas consecuencias perjudiciales procede jurídicamente atribuir al agente, es decir, pueden imputársele, de acuerdo con una serie de factores que obedecen más a valores y razones de política jurídica que a la existencia o ausencia real o efectiva de un vínculo causal¹⁵⁹. En este caso hablamos de “causalidad jurídica”, “imputación objetiva” o “alcance de responsabilidad” la cual permitirá atribuir un daño a una determinada persona.

Para ello doctrina y jurisprudencia acuden¹⁶⁰ a los criterios de la *previsibilidad* (sólo se responde del daño que una persona razonable y puesta en su posición hubiera previsto como resultado probable de su conducta) o el de la *adecuación* (como daño que resulta regularmente y de acuerdo con el curso normal de las cosas de la conducta o actividad desplegada)¹⁶¹. El denominado “sesgo de automatización”, que puede inducir al usuario profesional de una IA, en este caso al profesional médico, que responde de la correcta ejecución de las instrucciones facilitadas y de la supervisión del sistema, a no cuestionar esta tecnología o relajar el cumplimiento de este deber no puede por sí solo fundamentar una excepción que permita eximirle de responsabilidad frente a una demanda de responsabilidad civil, por supuesto siempre que se hayan cumplido los deberes de información por parte del fabricante y de formación

¹⁵⁹ MARTÍN-CASALS. M. “Acotaciones sobre la relación de causalidad y el alcance de la responsabilidad desde una perspectiva comparada, en SANTOS, M.J, MERCADER J.R. Y DEL OLMO, P. (Dir.), *Nuevos retos del Derecho de daños en Iberoamérica*, Valencia Tirant lo Blanch, 2020, 215-264.

¹⁶⁰ Otro expediente al que se recurre para superar estos inconvenientes partiendo de la previsibilidad o adecuación del daño es el de entender que será responsable aquel agente que, pudiendo hacerlo, no haya adoptado alguna medida o realizado alguna actividad para no incrementar los riesgos ordinarios de la vida que se materializarían en un daño en caso de la IA. Tomando en consideración el The Third Restatement of Torts: Liability for Physical and Emotional Harm § 29: “An actor’s liability is limited to those physical harms that result from the risks that made the actor’s conduct tortious.” Este criterio del “daño dentro del riesgo” supone que el agente responde de los daños que derivan de los riesgos que hacen que su conducta sea dañosa: un productor de IA respondería de acuerdo con este criterio de los daños y perjuicios acaecidos como consecuencia de la realización de un riesgo que es inherente al sistema inteligente de acuerdo con los dictados del diseño inicial, que permite que aquel altere su comportamiento sobre la base de experiencias posteriores. Resultado al que se llega del mismo modo aplicando la regulación de productos defectuosos, si bien en este caso se plantea como problema la determinación del estándar o parámetros de seguridad exigibles en cada supuesto.

¹⁶¹ PETL: Art. 3:201. Alcance de la responsabilidad: “Si una actividad es causa en el sentido de la Sección 1 de este Capítulo, la cuestión de si puede ser imputada a una persona y en qué medida depende de factores como los siguientes: a) la previsibilidad del daño para una persona razonable en el momento de producirse la actividad considerando, en especial, la cercanía en el tiempo y en el espacio entre la actividad dañosa y su consecuencia, o la magnitud del daño en relación con las consecuencias normales de tal actividad(...)”.

y capacitación tecnológica a cargo de la administración o centro sanitario en que presta servicios el profesional.

La aplicación a los sistemas de IA de este criterio de adecuación conduciría en muchos supuestos a que la víctima quedase sin indemnización por no poderse acreditar la causalidad desde el punto de vista jurídico: desde luego, en todos los de inteligencia fuerte con capacidades de autoaprendizaje de la máquina.

Y como se ha dicho anteriormente, en demasiados casos, puede resultar imposible en la práctica distribuir la responsabilidad de los distintos intervinientes en el proceso que termina con la comercialización e implementación de un robot, sistema o aplicación de IA sobre los que debe recaer la consecuencia indemnizatoria por referirse a ellos el juicio de imputabilidad: así, el *fabricante* podría deslindarse del *diseñador* de un producto, si bien para poder hablar de un “defecto de diseño”, éste debe afectar a todos los “lotes de productos” comparables, debiéndose realizar tal comparación con otros similares en el mercado para detectar el fallo, lo cual podría implicar la vulneración de los derechos de propiedad industrial (v.gr. el robot Da Vinci)¹⁶².

3.5. AGENTES IMPLICADOS EN LA PRESTACIÓN DE SERVICIOS MÉDICOS CON AUXILIO DE IA

A. El productor, fabricante o diseñador de la IA

Si bien no entraremos a analizar el régimen jurídico de responsabilidad por los daños por productos defectuosos¹⁶³, lo cierto es que el supuesto de

¹⁶² En cuanto al defecto de diseño, si tomamos en cuenta el criterio que utiliza el TRLGDCU basado en las “expectativas razonables del consumidor” dentro de los “usos previsibles” que se le pueden dar al producto para la apreciación del mismo, defraudada la legítima confianza del usuario del producto sanitario la responsabilidad será de carácter objetivo, pudiendo tal sólo invocar el fabricante o diseñador que el estado de los conocimientos científicos y técnicos existentes en el momento de su puesta en circulación no permitía apreciar la existencia del defecto (art. 140.1.e del TRLGDCU). Tomando como ejemplo el “Da Vinci”, y puesto que resulta acreditado estadísticamente que los riesgos del mismo no superan sus enormes beneficios, no sería posible probar tal defecto de diseño en la práctica porque las expectativas del consumidor partirán de un robot quirúrgico tecnológicamente avanzado y ampliamente implementado en la actualidad, resulta infinitamente menos arriesgado que los clásicos instrumentos quirúrgicos antes empleados por el cirujano humano.

¹⁶³ En cuanto a la responsabilidad del fabricante o diseñador de la IA, se plantea el problema de la determinación del agente u operador que haya causado tal daño resarcible por mal uso de un sistema IA, cuestión que, como señala ÁLVAREZ OLALLA, no resulta tarea sencilla, sobre todo cuanto más autónomo es un sistema. La doctrina distingue entre operador final o próximo y operador inicial. Aquel es la persona, física o jurídica, que ejerce el control sobre el riesgo asociado al funcionamiento de una IA, beneficiándose del mismo (“ubi emolumentum, ibi onus”): en este caso el médico o centro sanitario que se prevale de una IA. El “operador inicial” es el que define de modo

que el daño causado tenga su origen en un “defecto” en un sistema de IA como producto puede en la práctica constituir un supuesto que configura, en la opinión mayoritaria de la doctrina, un tipo de responsabilidad objetiva¹⁶⁴ del fabricante.

B. El “responsable del despliegue” usuario profesional

El perjudicado por daños causados por una actuación sanitaria en la que haya intervenido la IA podrá también, en su caso, articular la demanda de responsabilidad civil contra el profesional médico que haya intervenido, siempre que pueda fundamentarlo en la infracción de la “lex artis ad hoc”, así como contra el centro hospitalario y la aseguradora. Descartado por la UE el planteamiento de considerar la aplicación generalizada de un régimen de responsabilidad objetiva a todos los daños causados por la IA¹⁶⁵ el sistema se debe articular sobre principios subjetivos o de responsabilidad por culpa. Como es sabido, el motivo que fundamenta la articulación de sistemas de responsabilidad objetiva es la creación o incremento del riesgo de producción de daños¹⁶⁶ y este no es el sistema adecuado cuando se trata de tecnologías cuyos beneficios, en cualquier caso, superan los riesgos, sin perjuicio de la necesidad de prevenir éstos.

continuado las características de la tecnología, proporciona los datos, el servicio de apoyo final y, por lo tanto, ejerce también un grado de control (...)”. Tratándose de sistemas que implican un riesgo calificado normativamente como alto, la responsabilidad del productor, fabricante o diseñador del sistema de IA será objetiva o por el riesgo creado, por lo que no será necesario que el perjudicado pruebe la culpa, pero ello no exime de la carga de la prueba tanto del daño como de existencia de un vínculo de causalidad entre la acción u omisión del operador y el resultado dañoso.

¹⁶⁴ En contra, aquellos autores que cuestionan su carácter objetivo al requerirse la prueba del carácter defectuoso del producto. GUTIÉRREZ SANTIAGO (2008), op. cit., pág. 129, SALVADOR CODERCH y RAMOS GONZÁLEZ (2008), op. cit., pág. 77, Josep SOLÉ FELIU (2016), “La Directiva de la Unión Europea sobre responsabilidad por productos defectuosos: una perspectiva a la luz de la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas de los últimos 30 años”, Responsabilidad Civil y del Estado, núm. 38, pág. 129 e Isabel ZURITA MARTÍN (2021), “Capítulo 143. Gestión de riesgos y responsabilidad civil de los robots”, en ATAZ y CORBACHO GÓMEZ (Coords.), Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón, Tomo III, pág. 2013. GARCÍA MICÓ, T.G., Robótica quirúrgica y derecho de daños, Tesis Doctoral, Gómez Ligüerre. C.I (dir. tes.), Universitat Pompeu Fabra, Barcelona, 2022, cit. 238, p. 82.

¹⁶⁵ Salvo cuando se trate de productos defectuosos como se ha dicho, donde puede ser conveniente aplicar como criterio la necesidad de socializar tanto beneficios como pérdidas o costes.

¹⁶⁶ El art. 5: 101 PETL (“Principios de Derecho Europeo de la responsabilidad civil”) cuando se trata de actividades anormalmente peligrosas, la persona que las lleva a cabo responde objetivamente de los daños, no por culpa. Principios que desarrollan con carácter general lo dispuesto en el 1: 101 PETL, que establece que el daño puede imputarse a la persona cuya actividad anormalmente peligrosa lo haya causado (letra b), o a la persona “cuyo auxiliar lo haya causado en el ejercicio de sus funciones” (letra c).

Con base en el “principio de equivalencia funcional”, las víctimas de estos daños causados por IA son acreedoras del mismo trato que si se tratara de daños causados por humanos. El daño deber resarcirse, ya sea patrimonial o moral. Ahora bien: la responsabilidad del responsable del despliegue de una IA: ¿es una responsabilidad por hecho propio o configura un supuesto de responsabilidad por hecho ajeno? La aplicación de las reglas relativas a la responsabilidad civil por hecho ajeno resulta controvertida en derecho español; se dice que este enfoque parte de una “persona” como responsable directo de los daños de los que otra debe responder, presuponiéndose la personalidad o subjetividad de unos robots o sistemas de IA, que carecen. Si bien el tema resulta discutido en la doctrina, entiendo -negando la premisa- que la aplicación de las reglas de la responsabilidad “por hecho ajeno” no debe estar necesariamente supeditada al reconocimiento de la personalidad jurídica de los robots, tema obsoleto y cerrado ya a nivel comunitario. Coincidimos con CARRASCO¹⁶⁷ cuando afirma que se trata de responder objetivamente de la conducta subordinada de auxiliares (art. 1596 CC): en el ámbito de la responsabilidad civil contractual es indiferente que el sistema inteligente sea un auxiliar autónomo en el cumplimiento que el que constituya un mero instrumento para llevarlo a cabo. Los robots pueden ser desde el punto de vista dogmático inimputables, pero nada impide que puedan ser considerados, cuando de culpa contractual se trata, como agentes causantes de un daño resarcible

¹⁶⁷ CARRASCO PERERA, A. “A propósito de un trabajo de Gunter Teubner sobre la personificación civil de los agentes de inteligencia artificial avanzada (Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, Archiv für die Civilistische), Praxis, 218, 2018, pp. 155-205, Centro de Estudios de Consumo CESCO, publicaciones periódicas, 11 de enero de 2019, p. 3. Propone el autor reconocer a estos agentes al menos la capacidad jurídica necesaria para imputar la declaración negocial al principal a título de representante, mayormente para aislar al agente humano de la responsabilidad que conforme a Derecho civil no puede imputarse a un principal cuando el agente opera como un “falsus procurator” y al primero no se le puede atribuir la infracción de un deber de cuidado. En lo que respecta a la responsabilidad por incumplimiento contractual, (...) en términos prácticos no va más allá de lo que se llegaría negando toda imputación autónoma al agente robótico y predicarla directamente del gestor humano; porque en términos de responsabilidad contractual, es lo mismo que el agente humano responda del incumplimiento objetivamente por el riesgo de emplear determinados recursos para el cumplimiento o decir que el agente humano responde objetivamente de la conducta del agente artificial en cuanto ésta no es más que una conducta subordinada de auxiliares de cumplimiento, de los que se responde objetivamente (art. 1596 CC). No tiene importancia que en la dogmática jurídica se exija al menos culpa del auxiliar (en este caso, del autómatas), porque de hecho en materia contractual la culpa (*responsability*) se identifica con la simple ilicitud de la conducta de cumplimiento (*accountability*) y no aporta criterios adicionales para discriminar la responsabilidad. En el ámbito contractual da, pues, igual si el auxiliar en el cumplimiento es autónomo o si endosa la responsabilidad al principal como mero instrumento de cumplimiento. (...) En el ámbito extracontractual, el gestor del autómatas no estaría sujeto a una responsabilidad directa y primaria de naturaleza objetiva sobre la base del riesgo creado por el empleo de Inteligencia Artificial autónoma, sino a una responsabilidad vicaria por hecho de otro, incardinable en nuestro art. 1903 CC.

del que respondería el “principal” que se prevale o auxilia de ellos (art. 1903 CC¹⁶⁸).

Como afirma ATIENZA¹⁶⁹, ni la doctrina ni las normas comunitarias consideran hoy que la aplicación de las reglas de responsabilidad por hecho ajeno esté supeditada al reconocimiento de la personalidad jurídica de los robots: podría aún sin reconocérseles personalidad jurídica articularse una suerte de responsabilidad vicaria del principal por los hechos del auxiliar (NAVAS NAVARRO¹⁷⁰) lo que les haría ser imputables. En la actividad médica estos sistemas no dejan de ser elementos auxiliares o dependientes al servicio o en auxilio de personas físicas o jurídicas (centros hospitalarios privados o administraciones públicas) que se valen instrumental o auxiliarmente de ellos, obteniéndose indudables beneficios para el ejercicio de su actividad.

Enfocando la cuestión desde el prisma de la responsabilidad extracontractual, si consideramos la actividad médica, aun cuando hablemos de sistemas de alto riesgo, no puede eximirse el usuario profesional de responder por aquellos daños en los que haya intervenido culpa propia del profesional (art. 1902 CC) o culpa “in vigilando”, “in educando” (art. 1903 CC) de los sujetos llamados a responder: el diseñador, programador, entrenador y formador de un sistema inteligente deberían responder por ser quienes entrenan (educan, culpa “in educando”) la IA, y las personas (centros hospitalarios públicos o privados como personas jurídicas y médicos y profesionales de la salud como personas físicas) que se benefician del robot o sistema de IA en salud y lo utilizan para su actividad profesional responderían porque el sistema actúa subordinado a las órdenes o instrucciones de aquellos sujetos de derecho, personas físicas o jurídicas, que lo han elegido (responsabilidad “in eligendo”), incorporado a sus funciones, para obtener de ello ventajas (indudables) de su eficiencia (reducción de costes de todo tipo e incluso minimización de riesgos para los pacientes), en el sentido expuesto, estando por ello obligados a vigilarlo adecuadamente (responsabilidad “in

¹⁶⁸ A tenor del cual deben responder los dueños o directores de establecimientos o empresas respecto de los perjuicios causados por sus dependientes en el ejercicio de los ramos en que estuvieren empleados o con ocasión de sus funciones.

¹⁶⁹ ATIENZA NAVARRO, M^aL. “La responsabilidad civil por daños causados por inteligencia artificial: estado de la cuestión” en Derecho de contratos, responsabilidad extracontractual e inteligencia artificial, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024, p. 353. De la autora, “¿Daños nuevos, reglas nuevas para su indemnización? Responsabilidad civil e inteligencia artificial a la luz de las últimas Propuestas de la Unión Europea”, *Revista Aranzadi de derecho y nuevas tecnologías*, Núm. 4, 2024, *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, 2022.

¹⁷⁰ NAVAS NAVARRO, S. “Sistemas expertos basados en inteligencia artificial y responsabilidad civil. Algunas cuestiones controvertidas”, *La Ley Digital*, La Ley, 2019, p.6; *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022, p.29.

vigilando”). Por supuesto, ello sin perjuicio de la posibilidad de ejercicio de las acciones de regreso, en su caso.

Si se trata de daños causados por médicos en el ámbito de la sanidad pública, se aplicará la LRJSP, que establece una responsabilidad objetiva que exige probar que el daño se ha debido al “funcionamiento normal o anormal de los servicios públicos”: en cualquier caso no exime de tener que acreditar cumplidamente la relación de causalidad entre la acción u omisión y el resultado dañoso. Pongamos el ejemplo de un especialista en radiología de torax que se prevale de sistemas de IA débil (no autónoma) pero que, por su potencial, pueden aplicarse a prácticamente todas las fases del proceso de imagen clínica. Los radiólogos expertos afirman en este sentido que la IA puede ayudar a los clínicos a pedir la “mejor técnica” de imagen para cada paciente, mejorar las citaciones, mejorar la técnica radiológica disminuyendo tiempos o dosis de radiación o de contraste. Además resulta una ayuda para la función de diagnóstico médico¹⁷¹. Muchas de las herramientas de IA realizan tareas que típicamente hacen los médicos internos residentes (protocolizar, supervisar o preinformar los estudios radiológicos, segmentar y medir lesiones, etc.), de modo que las labores más repetitivas las ejecuta optimizando el rendimiento, pero no sería sensato que un residente confiara estas tareas a un software sin antes comprenderlas y saber realizarlas por sí mismo sin recurrir a la IA, de manera autónoma¹⁷².

El caso de un acto o intervención médica con auxilio de un sistema de IA “de alto riesgo” en el que el robot o sistema de IA tiene capacidad de adoptar decisiones autónomas actuando asolutamente desvinculado de la actuación del profesional sanitario es un escenario no permitido por el RIA.

Cuando hablamos de la IA como auxiliar de un médico, centro sanitario, hospital o plataforma que recluta profesionales, la responsabilidad es por hecho ajeno (art. 1903.4 CC), si bien actualmente la IA está evolucionando hacia

¹⁷¹ Se automatizan procesos que consumen mucho tiempo, segmentar lesiones o estructuras de interés en una imagen médica. Por otra parte, se puede extraer información de las imágenes imperceptible al ojo humano, analizarla de manera masiva con herramientas de “big data” y combinarla con otras fuentes de información, ayudando al diagnóstico pero también a la predicción de la evolución de un paciente o la detección temprana de anomalías que puedan desembocar en una patología (por ello se habla en este campo de la ‘inteligencia asistida’). DE LUIS, R. Redacción Médica: <https://www.redaccionmedica.com/secciones/radiologia/-la-inteligencia-artificial-esta-cambiando-todo-tambien-la-radiologia-2856>

¹⁷² Actualmente puede plantearse en qué medida y hasta dónde puede exigirse del profesional que se prevale o hace uso de estos dispositivos, tecnológicamente muy complejos, que se haga responsable de su correcto funcionamiento (¿dispone a la fecha el especialista en radiología de los conocimientos y habilidades necesarios para prevalecer de la IA en su función diagnóstica a través de imágenes?; ¿en qué medida y cuándo deben implementarse cambios en los planes de estudios universitarios para tal fin?).

este tipo de sistemas caracterizados por la capacidad de autoaprendizaje que, aun cuando partan de ciertas instrucciones iniciales, no siguen el esquema “principal-subordinado”¹⁷³ que permite aplicar los principios y esquemas de la responsabilidad vicaria.

En definitiva, habrá que estar a las circunstancias, que pueden ser muy distintas, de cada caso concreto. Al entrar a analizar la demanda de responsabilidad civil en un supuesto de daños causados en la prestación de servicios médicos con auxilio de la IA, el juez habrá que atender a los distintos escenarios posibles y a las singularidades de cada supuesto¹⁷⁴: respondería en algunos casos el fabricante o el desarrollador del dispositivo, sistema o robot sanitario de forma objetiva (es decir, exonerando al demandante de la prueba de la culpa, no de la relación de causalidad) en base al riesgo creado (responsabilidad objetiva o por riesgo), y en otros deberá hacerlo, por culpa, propia o ajena, el centro hospitalario o el profesional sanitario que se prevale de estos instrumentos beneficiándose de ello directa o indirectamente por no atenerse a las instrucciones de funcionamiento de tales máquinas y dispositivos tecnológicos, cuyo suministro es deber del fabricante o desarrollador, no interviniendo de forma directa en su control (“*back-end operator*”).

3.6. CAUSAS DE EXCLUSIÓN O EXONERACIÓN

Como causa de exclusión de responsabilidad del médico que se prevale de IA podrían citarse las interrupciones de suministro eléctrico (v.gr. por inundaciones, tormentas, terremotos u otros acontecimientos naturales) que podrían constituir una causa de exoneración si constituyen un supuesto de fuerza mayor siempre y cuando se hayan utilizado por los centros hospitalarios todas las medidas de prevención previstas normativamente.

¹⁷³ En estos casos, se ha llegado a plantear la atribución de una “personalidad jurídica electrónica” a los sistemas de IA considerados de alto riesgo: más allá de la excentricidad de la propuesta inicial, a la fecha descartada en la UE, desde el punto de vista práctico carece de todo sentido, toda vez que el resarcimiento pecuniario de los daños causados por robots a personas físicas no puede recaer sobre una máquina que, por muy inteligente y autónoma, carece de patrimonio propio, habiendo de dirigirse el acreedor contra el “bolsillo” de su fabricante o desarrollador (el que ha fabricado la máquina o diseñado el algoritmo), que respondería, de forma objetiva, en base al “*riesgo creado*” o conforme al principio “*ubi emolumentum ibi onus esse debet*”.

¹⁷⁴ En el ámbito sanitario, «*Las doctrinas sobre medicina curativa-medicina satisfactiva, y sobre obligación de medios-resultado (...) no se resuelven en respuestas absolutas, dado que según los casos y las circunstancias concurrentes caben ciertos matices y moderar las consecuencias. Las singularidades y particularidades, por tanto, de cada supuesto influyen de manera decisiva en la determinación de la regla aplicable y de la responsabilidad consiguiente (...)*» (STS 778/2009, de 20 de noviembre, ECLI:ES:TS:2009:6873).

Es posible plantearse si se rompe el nexo de causalidad en el caso de daños causados por actos de ciberdelincuencia o hackeos, que requieren la intervención de una conducta dolosa de terceros: entiendo que, menos en algunos estos casos podría imputarse responsabilidad al fabricante o diseñador del sistema por aplicación del mencionado criterio de adecuación y en base al diseño de un sistema hackeable, puesto que la posibilidad de hackeo es, como hipótesis fáctica en el orden de la técnica, algo previsible.

Una cuestión adicional es la relativa a la posibilidad de invocar como causa de antijuridicidad del daño o de exención de la culpa frente a una acción de responsabilidad civil los denominados “riesgos del desarrollo” o “riesgos del progreso tecnológico”, entendiendo por tal el estado de los conocimientos científicos o técnicos en el nivel más avanzado de las investigaciones que comprende todos los datos presentes en el circuito informativo de la comunidad científica en un determinado momento. En este sentido, la IA presenta como rasgo característico la esencial dinamicidad de sus aplicaciones: antes ya de comercializarse una aplicación o sistema se está trabajando en la próxima actualización o complemento que permite su mejora funcional. Si difícil es exigir al profesional médico estar, en cada caso en que interviene, “a la última” en lo que se refiere al “estado de la ciencia” (lo que le obligaría a dedicar su escaso tiempo libre a la consulta y estudio de las últimas publicaciones médicas de su especialidad), carece de razón pensar que deba en forma alguna ser experto en “Med Tech”, aun cuando se prevalga de ella, e incluso le beneficie, directa o indirectamente. Si bien entendemos que corresponde al responsable médico del despliegue de la IA, por ejemplo, el centro clínico u hospitalario la supervisión de los aspectos verificables de los sistemas de IA provistos, al disponer de guías y manuales de instrucciones, etc., la verificación de las correspondientes actualizaciones, mejoras, etc. corresponde a quienes conocen de primera mano su funcionamiento: el fabricante y/o el desarrollador de producto, ingeniero diseñador de la aplicación, producto sanitario o robot autónomo, que asumen la función de “*front end operator*” y que, por ello, en caso de materializarse un daño en el que no haya intervenido culpa o negligencia del usuario-paciente o profesional sanitario, debe responder, en este caso de forma objetiva en base al riesgo creado.

4. ALGUNAS REFLEXIONES SOBRE EL RÉGIMEN (NO ARMONIZADO Y “DE MÍNIMOS”) DE LA PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL A LA IA (PDRCIA)

En materia de responsabilidad extracontractual, la UE se ha decantado por abandonar las directrices contenidas en la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)). Sólo dos años después, la PDRCIA¹⁷⁵ no ha seguido la fórmula consistente en distinguir el fundamento subjetivo u objetivo de la responsabilidad según el riesgo, alto o no alto, del sistema de IA, sino que, provisionalmente al menos¹⁷⁶, aparca esta fórmula y parte de las reglas de responsabilidad por culpa contenidas en los (muy distintos) ordenamientos de los estados miembros (art. 23).

Se considera que un régimen general de responsabilidad objetiva puede suponer un freno a la innovación y al desarrollo tecnológico (lo cual no deja de ser cierto), desmotivando la necesaria inversión en este ámbito¹⁷⁷. Y además, que los sistemas de alto riesgo no se hallan actualmente tan extendidos (esto es ya más que discutible).

Por ello, recurre a expedientes procesales para facilitar la carga de la prueba a las víctimas: en particular la exhibición de pruebas y el régimen de presunciones) al expediente procesal de la presunción legal con carácter ‘iuris tantum’ (es decir, que admite prueba en contrario) en aquellos supuestos

¹⁷⁵ Comentarios valorativos acerca de esta propuesta normativa en ATIENZA NAVARRO, M^aL. “La responsabilidad civil por daños causados por inteligencia artificial: estado de la cuestión” en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024, pp. 380 a 398; muy riguroso el análisis que realiza PEÑA LÓPEZ, F. “Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la inteligencia artificial”, en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024, pp. 466 a 482.

¹⁷⁶ El régimen ha de ser escalonado o por fases a tenor de lo dispuesto en el art. 5. Para los primeros cinco años (plazo que ha sido considerado excesivamente amplio por el Comité Económico y Social Europeo que propone su reducción a 3, articula un sistema de exhibición de pruebas y de articulación de presunciones que admiten prueba en contrario (“iuris tantum”), con compromiso de reevaluar, transcurrido ese tiempo y a la vista de los cambios tecnológicos y siniestros acaecidos en la práctica, la necesidad de introducir un régimen de responsabilidad objetiva acompañándola de un seguro obligatorio.

¹⁷⁷ El régimen es de responsabilidad objetiva cuando se trata de daños causados por productos defectuosos: vid Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos 28.9.2022COM(2022) https://eur-lex.europa.eu/resource.html?uri=cellar:b9a6a6fe-3ff4-11ed-92ed-01aa75ed71a1.0015.02/DOC_1&format=PDF

de acciones de responsabilidad civil por daños causados por sistemas IA de alto riesgo (v.gr, diagnóstico por imágenes asistido por IA, robots quirúrgicos) cuando el tribunal considere que es excesivamente difícil para el demandante probar el nexo causal, o sistemas que no sean de alto riesgo (v.gr, chatbots médicos), cuando no hay pruebas suficientes razonablemente accesibles para el demandante.

Esta propuesta normativa establece para los sistemas de alto riesgo¹⁷⁸ una presunción “*iuris tantum*” (admite prueba en contrario) del nexo causal en caso de culpa: los jueces y tribunales están así facultados para presumir la existencia de nexo de causalidad entre la culpa del demandante y el resultado producido por el sistema de IA de alto riesgo o, en su caso, la ausencia de resultado, siempre y cuando:

- a) El demandante demuestre la culpa del demandado o;
- b) La parte actora no logre acreditar la culpa pero el tribunal la presume (prueba de presunciones), ya por no haber permitido el demandado el acceso a la información, ya no haberla preservado (art. 3.5 PDRCIA).

Según la norma, puede considerarse “razonablemente probable” que la culpa ha influenciado tanto el resultado producido por el sistema de IA como, en su caso, la ausencia del mismo. En este caso, se trata de aportar indicios para que se pueda aplicar la presunción legal.

La PDRCIA se aplica tanto si el demandado es el proveedor o un sujeto que debe cumplir con las obligaciones del proveedor o un usuario del sistema de IA: en este último caso, sin embargo, los deberes de cuidado que se consideran incumplidos son la obligación de usar o monitorizar el sistema de IA de alto riesgo de acuerdo con las instrucciones suministradas por el proveedor o, en su caso, suspender o interrumpir su uso, o exponer el sistema de IA a datos de entrada o inputs no relevantes para la finalidad perseguida por el sistema (art. 4.3). Sin embargo, esta presunción no se aplica si el demandante puede probar que existía suficiente información que estaba al alcance del demandante para probar los hechos en los que fundamenta su acción (art 4.4).

La PDRCIA y la PDRPD (responsabilidad por daños causados por productos defectuosos) constituyen sistemas normativos que difieren tanto por los sujetos y supuestos a los que se aplican como por los tipos de daños indemnizables: mientras el ámbito de aplicación de la primera se circunscribe a cualquier tipo de víctima y a cualquier tipo de daño indemnizable, la PDRPD

¹⁷⁸ En caso de sistemas de bajo riesgo, la presunción sólo se aplicará si los tribunales consideran excesivamente difícil para el demandante probar el mencionado nexo causal.

cubre la responsabilidad objetiva de los operadores económicos por daños causados por productos defectuosos, destinado a indemnizar a perjudicados que sean personas físicas por los daños contemplados en el art. 4.6: pérdidas materiales resultantes de daños personales, daños materiales sufridos por bienes destinados al consumo privado o mixto particular-profesional y de la pérdida de datos personales. En ningún caso pueden obtener resarcimiento a través de esta norma ni los daños morales puros o autónomos ni los derivados de intromisiones en derechos de la personalidad (v.gr intimidad, privacidad). Limitaciones que no existen en la PDRCIA, cuyas reglas están destinadas a la articulación de estos instrumentos de facilidad probatoria en las acciones de responsabilidad civil extracontractual por tipo de daños, personales y patrimoniales, si bien principalmente destinadas a aplicarse a los causados por sistemas de inteligencia artificial de alto riesgo. Por el momento, se trata de una propuesta de directiva comunitaria, que si llega a aprobarse, requerirá su trasposición a los ordenamientos de los estados miembros.

5. REFERENCIAS BIBLIOGRÁFICAS

- ALONSO SÁNCHEZ, A. “Los datos de salud en el marco de la medicina personalizada: perspectiva médica”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- ÁLVAREZ OLALLA, P. “Propuesta de Reglamento en materia de responsabilidad civil por el uso de inteligencia artificial, del Parlamento Europeo, de 20 de octubre de 2020”, *Revista CESCO de Derecho de Consumo*, N° 38, 2021.
- ATAZ LÓPEZ, J. “Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial”, *Càtedra Jean Monnet Working Paper*; 4/2020, Universidad de Murcia, agosto de 2020.
- ATIENZA NAVARRO, M^aL. “La responsabilidad civil por daños causados por inteligencia artificial: estado de la cuestión” en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024.
- “¿Daños nuevos, reglas nuevas para su indemnización? Responsabilidad civil e inteligencia artificial a la luz de las últimas Propuestas de la Unión Europea”, *Revista Aranzadi de derecho y nuevas tecnologías*, Núm. 4, 2024,
- *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, 2022.
- AVILA TOMAS, J.F.; MAYER PUJADAS, M.A.; QUESADA VARELA, V.J.; “La inteligencia artificial y sus aplicaciones en medicina: importancia actual y aplicaciones prácticas, *Atención Primaria*, vol. 53, n.º.1, 2020.

- BADILLO ARIAS, J.A; ÁLVAREZ OLALLA, P; DÍAZ DÍAZ, E. *Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento. Responsabilidad civil y aseguramiento obligatorio de los robots*, Tirant lo Blanch, Valencia, 2019.
- BARRIO ANDRÉS, M.; FROOMKIN A. MICHAEL. *Derecho de los robots*. Wolters Kluwer España, S.A. La Ley, Madrid, 2018.
- BARRIO ANDRÉS, M. “Hacia una personalidad electrónica para los robots”. *Revista de derecho privado*, 2018; BARRIO ANDRÉS, M., FROOMKIN A.M. *Derecho de los robots*. Wolters Kluwer España, La Ley, Madrid, 2018.
- BENAVENT NÚÑEZ, D. COLOMER MASCARÓ, J. et al, *Inteligencia Artificial y decisiones clínicas: cómo está cambiando ello comportamiento médico*, Fundación Gaspar Casal, 2020.
- BLOOM, SALZBERG & KRUMMEL (2002). <http://www.medicalexpo.com/prod/lut/endoscopes-rigid-right-angled-laparoscopes-working-channel>
- BUSTINCE SOLA, H., “Caminos hacia la superinteligencia”, en LLEDÓ YAGÜE, F., BENÍTEZ ORTÚZAR, I., MONJE BALMASEDA, O., (dirs.) *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, 2021.
- BUSTO LAGO, J.M. “Digitalización de la salud, responsabilidad civil y seguro”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- CARRASCO PERERA, A. “A propósito de un trabajo de Gunter Teubner sobre la personificación civil de los agentes de inteligencia artificial avanzada (Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagentem, Archiv für die Civilistische), Praxis, 218, 2018, Centro de Estudios de Consumo CESCO, publicaciones periódicas, 11 de enero de 2019
- CID, YASHIN DICENTE et al., “Development and validation of open-source deep neural networks for comprehensive chest x-ray reading: a retrospective, multicentre study”, *The Lancet Digital Health*, Vol. 6, Issue 1, e44 - e57, enero 2024.
- DE MIGUEL ASENSIO, P.A., “Propuesta de Reglamento sobre Inteligencia Artificial”, *La Ley Unión Europea*, núm. 92, mayo 2021.
- DE MIGUEL BERIAIN, I. “Medicina personalizada, algoritmos predictivos y utilización de sistemas de predicción automatizados en asistencia sanitaria: problemas éticos”, *Dilemata*, n° 30, 2019, p.96.
- DÍAZ ALABART, S. *Robots y Responsabilidad civil*, Reus, Madrid, 2018.
- EBERS, M. “Terapia sin terapeutas”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- “Transparenz und Erklärbarkeit”, en EBERS, M. (ed.), *Legal Tech Stichwort kommentar; Recht - Geschäftsmodelle-Technik*, Nomos, Baden-Baden, 2023, EBERS, M. “Standardizing AI - The Case of the European Commission’s Proposal for an Artificial Intelligence Act”, en DIMATTEO, L. A., PONCIBÒ, C. y CANNARSA,

- M. (eds.), *"The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics"*, Cambridge University Press, Cambridge, 2022.
- EBERS M, HOCH VRS, ROSENKRANZ F, RUSCHEMEIER H, STEINRÖTTER B. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J.* 2021; 4(4):589-603. <https://doi.org/10.3390/j4040043>
- EVANGELIO LLORCA, R. "Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE" en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024.
- FERNÁNDEZ COSTALES, J., "Estado actual de la casuística de la responsabilidad sanitaria", en MORENO MARTÍNEZ, J. A. (Coord.), *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007.
- FERNÁNDEZ HERNÁNDEZ, C. "La OCDE explica el contenido de su definición actualizada de los sistemas de Inteligencia Artificial", Diario La Ley 06/03/2024, <https://diariolaley.laleynext.es/dll/2024/03/07/la-ocde-explica-el-contenido-de-su-definicion-actualizada-de-los-sistemas-de-inteligencia-artificial>
- FOSCH-VILLARONGA, E. y ÖZCAN, B., "The progressive intertwining Between Design, Human Needs and the Regulation of Care technology: The Case of Lower-Limb Exoskeletons", 2020;
- FOSCH-VILLARONGA, E. y GOLIA, A. Jr, "Robots, standards and the law: Rivalries between private standards and public policy making for robot governance", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2019.
- GARCÍA MICÓ, T.G, *Robótica quirúrgica y derecho de daños*. Tesis Doctoral, Gómez Ligüerre. C.I (dir. tes.), Universitat Pompeu Fabra, Barcelona, 2022.
- "Litigación asociada a la cirugía robótica con el Da Vinci", *Indret Revista para el Análisis del Derecho*, octubre de 2014.
- GARCÍA-PIETO CUESTA, J. «¿Qué es un robot?», en BARRIO ANDRÉS, M. (Dir.), *Derecho de los robots*, 2ª edición, Wolters Kluwer, Madrid, 2019.
- GARCÍA VICENTE, J.R. "Notas sobre *lex artis ad hoc*" y responsabilidad médica", LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- GIL MEMBRADO, C. (Dir.). "Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra", en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024.
- "En el horizonte: la Directiva de responsabilidad extracontractual en materia de IA" / Gil Membrado, C. en *Derecho y Medicina: Desafíos Tecnológicos y Científicos*, Dykinson, Madrid, 2023.
- *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, (Dir.) Reus, Madrid, 2023

- “Una nueva era hacia el robot sanitario “autónomo” y su encaje en el Derecho”. En Bioderecho y retos. M-Health, genética, IA, robótica y criogenización /Cristina Gil Membrado (dir.), Dykinson, 2022.
- “Una asignatura pendiente: la regulación de la prestación sanitaria a través de telemedicina”, en *El nuevo marco legal del teletrabajo en España*, Bosch, Madrid, 2021.
- JORQUI AZOFRA, M. “El EED y algunas cuestiones relativas a la licitud del uso secundario de los datos sanitarios”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia 2024.
- *Responsabilidad por los daños causados por productos y sistemas de Inteligencia Artificial*, Dykinson, Madrid, 2023.
- LEON RODRIGUEZ, H., “Sistema macro & micro robótico para aplicaciones médicas”, *Revista de Tecnología*, vol. 16, n° 2, pp. 104-113, 2019.
- MADIEGA, A., “Artificial Intelligence Act, Briefing”, 2 de septiembre de 2024. [https://www.europarl.europa.eu/thinktank/es/document/EPRS—BRI\(2021\)69879](https://www.europarl.europa.eu/thinktank/es/document/EPRS—BRI(2021)69879)
- LLEDÓ YAGÜE, F., *Los nuevos esclavos digitales del siglo XXI y la superación del hombre óptimo ¿Hacia un nuevo derecho robótico?*, Dykinson, 2022.
- LÓPEZ TUR, T. “Aplicaciones móviles de salud y protección de datos personales” en GIL MEMBRADO, C. *Bioderecho y retos. M-Health, genética, IA, robótica y criogenización*, Dykinson, 2022.
- LUQUIN BERGARECHE, R. “Aplicaciones y dispositivos de evaluación de síntomas en salud digital: aproximación jurídica”, en GIL MEMBRADO, C. y LUQUIN BERGARECHE, R. (Dir.) *Salud digital. aplicaciones móviles, telemedicina y chatbots*, Dykinson, 2024.
- “La Digitalización de los servicios de salud: implicaciones jurídicas de un nuevo paradigma”, en LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024;
- “Salud Digital a través de plataformas y otros prestadores de servicios: aproximación a un nuevo paradigma de Paciente Digital”, en GUIMARÃES, M.R /RUTE TEIXEIRA, P. *Direito e Inteligência Artificial*, Almedina, Coimbra, julio, 2023.
- MARTÍN CASALS, M. “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”, *Indret*, 3/2023.
- “Acotaciones sobre la relación de causalidad y el alcance de la responsabilidad desde una perspectiva comparada, en SANTOS, M.J, MERCADER J.R. Y DEL OLMO, P. (Dir.), *Nuevos retos del Derecho de daños en Iberoamérica*, Valencia Tirant lo Blanch, 2020.
- “Causation and Scope of Liability in the Internet of Things” en SEBASTIAN LOHSSE /REINER SCHULZE/DIRK STAUDENMAYER (EDS) *Liability for Artificial Intelligence and the Internet of Things*, Nomos Verlag, Baden Baden, 2018.

- MARTÍNEZ NAVARRO, J.A. *El Régimen Jurídico de la Salud Electrónica*, Tirant lo Blanch (Monografías), Valencia, 2018.
- MAZZILLI, E. “La vulnerabilidad negocial del consumidor: una referencia particular al caso de los servicios sanitarios prestados a través de los medios digitales”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- NAVAS NAVARRO, S., *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*, Comares, Granada, 2022.
- “Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial”, *Revista CESCO de Derecho de Consumo*, núm. 44, 2022;
- “Sistemas expertos basados en inteligencia artificial y responsabilidad civil. Algunas cuestiones controvertidas”, *La Ley Digital*, La Ley, 2019;
- NAVAS NAVARRO, S.; GÓRRIZ LÓPEZ, C.; CAMACHO CLAVIJO, S., et al., *Inteligencia artificial, Tecnología y Derecho*, Tirant lo Blanch, Valencia, 2017.
- NÚÑEZ ZORRILLA, M. C., *Inteligencia artificial y responsabilidad civil: régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*. Colección Scientia jurídica, Reus, Madrid, 2019.
- PEÑA LÓPEZ, F. “Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la inteligencia artificial”, en *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Álvarez Lata (Coord.), APPDC, Aranzadi, 2024.
- RAMON FERNÁNDEZ, F., “La inteligencia artificial y la medicina: médicos robots o robots médicos?”, *Revista Chilena de Derecho y Tecnología*, vol. 10, n.º. 1, 2021.
- REGLERO CAMPOS, L.F. Y MEDINA ALCOZ, L. “El nexo causal. La pérdida de oportunidad. Las causas de exoneración de responsabilidad: culpa de la víctima y fuerza mayor”. REGLERO CAMPOS, L.F. (COORD.), BUSTO LAGO J.M.(coord.), *Tratado de responsabilidad civil*. Thomson Reuters Aranzadi, 2014.
- RUDA GONZÁLEZ, A. “E-Health Big Data: Perspectiva Comparada (Cataluña-Japón)”, en LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- SENIGAGLIA, R. “E-Health en la Unión Europea. Las prácticas de telemedicina en el marco normativo italiano y en el personalismo de la relación asistencial”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- SOLÉ FELIU, J. “Responsabilidad civil y telemedicina: el valor de las guías de práctica clínica y protocolos en la determinación del estándar de diligencia”, LUQUIN BERGARECHE, R. (Dir.) *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, Valencia, 2024.
- TORAL LARA, E. “La prestación de servicios de salud digital y la responsabilidad por incumplimiento: especial referencia a la telemedicina”, LUQUIN

- BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, 2024.
- TORRELLES TORREA, E. “Telemedicina y pacientes vulnerables”, LUQUIN BERGARECHE, R. *Servicios Privados de Telemedicina y Salud Digital: desafíos e implicaciones jurídicas*, Tirant lo Blanch, 2024.
- TAYLOR, R. H.; STULBERG, S.D. *Medical robotics working group section report. Proc. NSF Workshop Medical Robotics and Computer-Assisted Medical Interventions (RCAMI)*, 1996.
- TUR FAÚNDEZ, M.N. “E-salud, derecho a la información y consentimiento informado”, en GIL MEMBRADO, C. (Dir.) *Bioderecho y Retos. M-health, Genética, IA, Robótica y Criogenización*, Dykinson, Madrid, 2021.
- ZAPATA SEVILLA, J. *Inteligencia artificial y responsabilidad civil: el caso de las organizaciones descentralizadas autónomas*. La regulación de los algoritmos, Cizur Menor, Thomson Reuters Aranzadi, 2020.
- ZURITA MARTÍN, I. “Capítulo 143. Gestión de riesgos y responsabilidad civil de los robots”, en Joaquín Ataz y José Antonio Corbacho Gómez (Coords.), *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón*, Tomo III, 2021.
- *Responsabilidad por daños causados por robots inteligentes como productos defectuosos*, Reus, Madrid, 2020.

La doctrina *crashworthiness*: origen, desarrollo y posible aplicación a los vehículos automatizados^{1/2}

ANDRÉS MARÍN SALMERÓN

*Profesor Ayudante Doctor de Derecho civil
Universidad de Murcia*

Sumario: 1. La doctrina *crashworthiness* o *second collision*. 1.1. Breve referencia a su concepto y objetivo del trabajo. 1.2. Principios y orígenes de la doctrina *crashworthiness*. 1.2.1. *Evans v. General Motors Corp.* 1.2.2. *Larsen v. General Motors Corp.* 1.2.3. *Dreisontok v. Volkswagenwerk, A. G.* 1.3. Aplicación de la doctrina *crashworthiness*. Relación de la primera colisión con la *second collision*: intervención de tercero y culpa del perjudicado. 1.3.1. La relevancia de las circunstancias de la primera colisión. 1.3.2. La doctrina mayoritaria. 1.3.3. La doctrina minoritaria: *D'Amario v. Ford Motor Co.* 1.3.4. Problemática probatoria y de desarrollo de la doctrina *crashworthiness*. 2. Su conexión con el criterio de riesgo-utilidad y el diseño alternativo razonable: de nuevo con la responsabilidad subjetiva. 3. La doctrina *crashworthiness* en la jurisprudencia española. 4. La aplicación de la doctrina en España: su compatibilidad con el Real Decreto Legislativo 8/2005, de 29 de octubre por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor. 5. La aplicación de la doctrina *crashworthiness* con la nueva normativa de responsabilidad por daños por productos defectuosos. 6. Bibliografía.

¹ Este trabajo ha sido elaborado en el marco del Proyecto PGC2018-098206-B-I00 «El Derecho de contratos en el entorno digital» financiado por el Ministerio de Ciencia, Innovación y Universidades y cuyas investigadores principales son Isabel González Pacanowska y María del Carmen Plana Arnaldos.

² El presente trabajo contiene múltiples traducciones de textos ingleses que se han traducido al español por el propio autor.

1. LA DOCTRINA *CRASHWORTHINESS* O *SECOND COLLISION*

1.1. BREVE REFERENCIA A SU CONCEPTO Y OBJETIVO DEL TRABAJO

La doctrina americana denominada *crashworthiness* o *second collision* está conectada principalmente con los defectos de diseño³. Y en concreto, en el ámbito del diseño de los vehículos a motor. Aunque en un principio sólo se dio en automóviles, la regla se ha ido extendiendo progresivamente a otro tipo de vehículos a motor como tractores, motocicletas⁴, aviones, barcos⁵, buques, hasta máquinas y estructuras industriales⁶, e incluso existe algún caso donde se ha planteado en un cortacésped^{7 8}.

³ Viene recogida en el art. 16 del *Restatement (Third) of torts: Products Liability*, al señalar que «un factor sustancial en el aumento del daño de los demandantes más allá de lo que habría resultado de otras causas, el vendedor del producto está sujeto a responsabilidad por este aumento del daño», señalando también que «aunque los accidentes no son usos intencionados de los productos, generalmente son previsibles. Un fabricante tiene el deber de diseñar y fabricar su producto para reducir razonablemente el daño previsible que puede ocurrir en un accidente provocado por causas distintas a un defecto del producto». Vid. BUBLICK, E. M., «The Tort-proof plaintiff the drunk in the automobile, *Crashworthiness* claims, and the restatement (third) of torts», *Brooklyn Law Review*, n° 3, 2009, pp. 711 y ss.

SHAPO, M. S. A., *Shapo on the law of products liability*, Edward Elgar, 7ª edición, 2017, pp. 9-89, ya señaló que, aunque algunos estén intentando justificar un desuso de la doctrina amparándose en la falta de uso de los términos concretos, es decir, aunque no se utilice la expresión *crashworthiness*, los principios de la doctrina se siguen utilizando de la misma manera. Menciona en su argumentación la sentencia *Roe v. Deere Co.* 855 F.2d 151 (3d Cir. 1988) que al tratar un caso de accidente referente a un tractor en el que se declaró que una protección antivuelco (ROPS) habría protegido al dañado, indicó que la alegación de la condición defectuosa del tractor ya fue suficiente para introducir los elementos necesarios de aplicación de la doctrina *crashworthiness*. Vid. también al respecto *Dept. of Gen. Servs v. US. Mineral Prods Co.* (898 A.2d 590, 600 (Pa. 2006)).

⁴ Algunas de las primeras sentencias donde empezó a extenderse la doctrina *crashworthiness* a las motocicletas fueron *Nicolodi v. Harley-Davidson Motor Co.* (70 So. 2d 68 (Fla. Dist. Ct. App. 1979)). Y *Bolm v. Triumph Corp.* 71 A.D.2d 429 (N.Y. App. Div. 1979) que desarrollaremos más adelante.

⁵ Como ocurre en el caso *Rose v. Mercury Marine Div. Of Brunswick Corp.*, (483 So. 2d 1351 (Miss. 1986)), donde el Tribunal de Mississippi aplicó la doctrina *crashworthiness* a un caso de barco a motor. Ante la posibilidad de una inminente colisión, el conductor del barco apagó el motor, sin embargo, la hélice siguió funcionando, produciéndose el accidente. El demandante alegó que se trataba de un caso de *crashworthiness*.

⁶ Vid. *Habecker v. Clark Equip. Co.* (942 F.2d 210 (3d Cir. 1991)). También es cierto que en algunas ocasiones se ha planteado la aplicación de la doctrina *crashworthiness* en supuestos que no se referían a vehículos motorizados, normalmente con resultados idénticos. Cabe destacar el caso *Jackson v. York Hanover Nursing Centers* (876 So. 2d 8 (Fla. 5th DCA 2004)), en el que el accidente provocó los daños que supusieron la muerte de un anciano en una residencia por deshidratación, y donde se intentó separar esta de una posible negligencia médica. Es reseñable la afirmación que realizó el tribunal al declarar que «a diferencia de los accidentes automovilísticos que involucran daños que surgen únicamente de la colisión en sí, la responsabilidad del acusado en un caso de *crashworthiness* se basa en la existencia de una lesión distinta y secundaria causada por un producto defectuoso, asumiendo que el demandante se encuentra en una condición distinta y posterior a la del «primer accidente». Por

Su mayor campo de aplicación se ha dado en el automóvil, enfatizándose en cinco grandes áreas diferenciables: (a) estructura del automóvil, siendo esta la capacidad del mismo de mantener el espacio habitable para ocupantes durante toda la secuencia del choque; (b) contención-retención de ocupantes dentro del espacio habitable durante la secuencia o transcurso de la colisión; (c) entorno de aceleración del ocupante, pudiendo definirse como la tasa de inicio, magnitud, duración y dirección de las aceleraciones experimentadas por los ocupantes como resultado del accidente; (d) peligros posteriores al choque, es decir, la amenaza a la supervivencia de los ocupantes planteada por un posible estallido que dé lugar a fuego en el vehículo tras el impacto; y por último, (e) peligros medioambientales, como barreras, proyecciones y equipo suelto que ocasione daños durante la secuencia del choque⁹.

De acuerdo con los ideadores de esta teoría¹⁰, el productor de un automóvil, que no es el causante inicial de un accidente, debe responder por

lo tanto, los casos de resistencia al choque (*crashworthiness*) involucran lesiones separadas y distintas: las causadas por la colisión inicial y las causadas posteriormente por una segunda colisión derivada de un producto defectuoso. Estamos de acuerdo en que, visto desde este punto de vista, los casos de *crashworthiness* pueden ser análogos a los casos de negligencia médica que involucran a un proveedor médico negligente sucesivo que supuestamente agravó una lesión existente o causó una lesión separada y adicional». De igual forma, la sentencia *Sta-Rite Industries, Inc. (V. Levey. 909 So.2d (Fla. 3d DCA 2005))* versa sobre el ahogamiento de un adolescente mientras disfrutaba de un baño en una piscina. El adolescente quedó atrapado por la succión del drenaje de la piscina. Para cuando finalmente fue rescatado, los daños eran irreversibles. El demandante alegó que los daños se produjeron por dos accidentes distintos. El primero cuando su brazo quedó atrapado por la succión del drenaje de la piscina, y el segundo porque no se pudo liberar de la succión, tal y como habría ocurrido si el dispositivo que impide dicha succión hubiese sido debidamente instalado. En ambos casos se declaró la inexistencia de dos accidentes. Vid. en este sentido SHAPO, M. S. A., *Óp. Cit.*, 2017, pp. 9-89.

⁷ Vid. *Tafuya v. Sears, Roebuck & Co. 884 F. 2d. 1330, 1337 n. 14 (10th Cir. 1989)* donde el Tribunal señaló la existencia de pruebas sustanciales de lesiones resultantes del contacto con las hojas giratorias de las cortadoras de césped, observando que el riesgo de lesiones graves en estos casos era bastante grande. Se confirmó que los productores de estas cortadoras no podían ser eximidos de la aplicación de la doctrina *crashworthiness*. Y también *Malen v. MTD Prods, Inc., 628 F.3d 296 (7th Cir. 2010)* donde citando la *CONSUMER PRODUCT SAFETY COMMISSION, RIDING LAWN MOWERS* señala que los accidentes de cortacésped son previsible al igual que ocurre con los accidentes en carreteras.

⁸ Aunque el objeto del trabajo se circunscribe a los vehículos automatizados, en el caso de que fuese extrapolable la doctrina *crashworthiness* a los accidentes en los que se vean implicados este tipo de productos, no sería extraño inferir las mismas consideraciones en la automatización del resto de vehículos, como son los aviones, trenes, buques, etc. Vid. YEOMANS, G., «Autonomous vehicles: handing over control», *Lloyd's of London*, 2014, pp. 5 y ss; LEVALLEY, D., «Autonomous vehicle liability. Application of common carrier liability», *Seattle University School of Law Digital Commons*, n° 36, 2013 pp. 5 y ss; o, COLONNA, K., «Autonomous Cars and Tort Liability», *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 4, n° 4, 2012.

⁹ Vid. GALERSTEIN G., «A review of Crashworthiness», *Journal of Air Law and Commerce*, vol. 45, n° 1, 1979, p. 194; y NADER, R. «Automobile Design Hazards», *AM. JUR. Proof of Facts*, 1965.

¹⁰ Vid. entre otros LAWRENCE MACDOUGALL, V., *Products Liability Law in Oklahoma*, Austin-Texas, Butterworth Legal Publishers, 1990, p. 242; y MADDEN M. S., «Products Liability», *St. Paul*

los daños causados a terceros o a los ocupantes del vehículo siniestrado que resulten de la denominada «segunda colisión». Aludiendo esta expresión al impacto que sufren en estos supuestos los ocupantes del vehículo contra su interior, o al impacto producido por su posterior expulsión al exterior, todo ello como consecuencia de la «primera colisión». Los productores sólo pueden ser considerados responsables por las lesiones que se han agravado por la existencia de un defecto de diseño en el producto¹¹, defecto que podría concretarse en la insuficiente resistencia del vehículo frente al choque (*crashworthiness*)¹².

La particularidad de esta doctrina reside en que, en este caso, el defecto de diseño en el vehículo no ha sido la causa principal ni inicial del daño, sino que ha contribuido a agravar los daños que, de igual manera, se hubieran producido. La insuficiente resistencia de un vehículo frente al choque (literalmente *crashworthiness*) constituiría pues un particular defecto. La cuestión principal aquí es conocer si el productor/diseñador debe responder por los daños que se han producido o por los daños agravados a partir de la «segunda colisión»¹³.

En este momento, la irrupción de los vehículos automatizados o semiautomatizados es ya una realidad, y se prevé que su desarrollo continúe de manera exponencial¹⁴. Las ventajas en la fabricación, comercialización y uso de estos

Minn. West Publishing Co., 1988, pp. 306 y ss. En España Vid. SOLÉ i FELIU, J., *El Concepto de defecto del producto en la responsabilidad civil del fabricante*, Tirant lo Blanch, Valencia, 1997, pp. 233 y ss.

¹¹ Vid. HOENIG, M.; y WERBER, S. J., «Automobile Crashworthiness: An Untenable Doctrine», *Cleveland State Law review*, vol. 20, n° 3, 1971, pp. 578.

¹² July, W. P.; OWEN, D. G.; MONTGOMERY, J. E.; y GREEN, G. *Products Liability and Safety. Cases and Materials*, 2nd, Westbury-New York, The Foundation Press, 1989, pp. 789 y ss.

¹³ Vid. PROSSER, W. L., *Law of Torts*, 4ª ed., 1971; y ROTH, L. M., «Florida Supreme Court Needs a Second Look at Second Collision Motor Vehicle Cases», *Florida Bar Journal*, vol. 78, abril, 2004. Cuestión diferente es el caso en el que la introducción por parte del comprador de un elemento externo en el diseño del vehículo haya sido el motivo del agravamiento de los daños. Este es el supuesto de la SAP de La Coruña de 15 de mayo de 2017 (LA LEY 82036/2017). En ella se discuten los daños que se han producido al activarse los *airbags* de un coche policial por los golpes realizados por un detenido en el interior del vehículo. El productor intenta reducir su responsabilidad indicando que la implantación de una mampara en el interior del vehículo pudo agravar los daños que se produjeron a las personas que se encontraban en el interior del vehículo cuando los *airbags* se activaron. El juez no tuvo en cuenta este argumento puesto que no se llegó a practicar prueba sobre esta cuestión. Vid. también FOLAND, W. J., «Enhanced Injury: Problems of Proof in Second Collision and Crashworthy Cases», *Washburn Law Journal*, vol. 16, 1977.

¹⁴ Como indica LÓPEZ MAS, P. J., «La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento», *Revista Crítica de Derecho Inmobiliario*, n° 801, 2024, pp. 61 y ss, el uso de la expresión «vehículo autónomo» es más propio de medios de divulgación, acercándose más a una definición correcta el concepto de «vehículo automatizado». De hecho, como indica el autor, el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación del tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes

novedosos medios de transporte se concretan en la liberación de recursos y en el aumento de la producción de las personas durante sus desplazamientos, en la eliminación de los obstáculos que la conducción tradicional acarrea para ciertos colectivos y, sobre todo, en la presunta reducción de siniestralidad que conllevará su aparición en las carreteras de todo el mundo¹⁵. Sin embargo, no parece razonable pensar en la eliminación total de los accidentes, ni siquiera, aunque la totalidad de los vehículos utilizado sean de estas características¹⁶. Es necesario, por tanto, la búsqueda de métodos que faciliten el resarcimiento de los daños producidos ante accidentes donde estén involucrados vehículos semiautomatizados o automatizados, y el criterio ideado con la doctrina *crashworthiness* puede servir a esta labor. Este es el objetivo de este trabajo: explorar si, con carácter general, alguna de las vertientes de la doctrina *crashworthiness* es aplicable a los supuestos de accidentes de vehículos automatizados independientemente de su nivel de automatización¹⁷.

de los vehículos y de los usuarios vulnerables de la vía pública, contiene una definición de «vehículo automatizado», frente al de «vehículo totalmente automatizado», que sería el popularmente conocido como «autónomo». Por el contrario, algunos autores como ELIZALDE SALAZAR, I., *Vehículos autónomos. Responsabilidad civil y seguro*, Thomson Reuters Aranzadi, 2022, pp. 36, atendiendo al estándar J3016 publicado por la *Society of Automotive Engineers* (SAE), entienden que los vehículos con características de los niveles 2, 3 y 4, es decir, aquellos que contienen algún dispositivo que les permite la realización de ciertas operaciones en la conducción de manera automática, son los que debemos conocer como «vehículo automatizado», pero no como autónomos; mientras que autónomos sería solo los que cumplan con los requisitos del nivel 5, es decir, aquellos en los que la totalidad de las operaciones de conducción se realizan de manera autónoma y prescindiendo de cualquier grado de intervención humana. En el mismo sentido señala IZQUIERDO GRAU, G., «La responsabilidad del productor de vehículos autónomos en el marco de la (futura) legislación en materia de responsabilidad por daños causados por productos defectuosos», *Revista de Derecho Civil*, vol. 10, n° 2, 2023, pp. 119 y ss, que aunque distinguiendo entre «vehículo autónomo» y «vehículo totalmente autónomo». Por otro lado, NÚÑEZ ZORRILLA, C., «La nueva directiva europea sobre responsabilidad civil por productos defectuosos y su aplicación a los vehículos totalmente automatizados o autónomos», *Revista Crítica de Derecho Inmobiliario*, n° 796, 2023, pp. 809 nos habla también de la «conducción altamente automatizada».

¹⁵ Desarrolla profundamente estas ventajas y beneficios ELIZALDE SALAZAR, I., *Óp. Cit.*, 2022, pp. 44 y ss. Respecto a la menor reducción de siniestralidad existen estudios que descartan una relación directa *vid.* FAVARO, M.; NADER, N.; EURICH, S. O.; TRIPP, M.; VARADARAJU, N., «Examining accident reports involving autonomous vehicles», *Plos One*, 12 (9), 2017.

¹⁶ Como indica MACANÁS VICENTE, G., «Mutualización de los riesgos generados por los sistemas de IA», *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial* (Coord. Álvarez Lata, N.), Aranzadi, 2024, p. 693, la incorporación cotidiana de sistemas de IA nos generará inevitablemente incertidumbre en sus actuaciones, y con ella, la sombra del riesgo. Agrega, además, que entre las muchas incertidumbres relativas a la implantación y sus efectos, jurídicos y sociales, sí existe una certeza inevitable y es que las IAs provocarán daños. Añade ORTIZ FERNÁNDEZ, M., *La responsabilidad civil derivada de los daños causados por sistemas inteligentes y su aseguramiento*, Dykinson, 2021, p. 36, que una de las peculiaridades de los sistemas de IA es, precisamente, el desconocimiento y la ausencia de certezas sobre el funcionamiento real de estas máquinas.

¹⁷ Como hemos indicado existen diversas clasificaciones atendiendo al nivel de autonomía de los vehículos, sin embargo, la más popular y reconocida es el estándar J3016 publicado por la *Society of*

1.2. PRINCIPIOS Y ORÍGENES DE LA DOCTRINA *CRASHWORTHINESS*

1.2.1. *Evans v. General Motors Corp*

Como gran parte de las teorías relativas a la responsabilidad civil por productos defectuosos, los comienzos de la doctrina *crashworthiness* tienen su origen en Estados Unidos¹⁸. La primera ocasión en la que se habló de esta doctrina fue en la sentencia *Evans v. General Motors Corp.* (359 F.2d 822 (7th Cir. 1966)), donde simplemente se mencionó, ya que finalmente se consideró que, a la hora de diseñarse un vehículo, no tenía por qué considerarse el riesgo que supondría que ese vehículo participase en un siniestro¹⁹. En el caso concreto había fallecido el conductor de una camioneta Chevrolet al ser golpeada lateralmente por otro vehículo. El vehículo que recibió el golpe había sido diseñado con un marco en forma de «X» que carecía de rieles laterales que protegieran al conductor ante este tipo de impactos. Los abogados de *General Motors* argumentaron que el uso normal de un vehículo no incluía su participación en colisiones con otros objetos, por lo que se debía diseñar un automóvil pensando en el uso adecuado del vehículo, sin defectos ocultos que hiciesen peligrosa su conducción, pero sin que tuvieran el deber de hacer un vehículo «a prueba de accidentes o infalible»²⁰. El Tribunal razonó que «el propósito de un automóvil no incluye su participación en colisiones con otros objetos, a pesar de la capacidad del fabricante de prever la posibilidad de que tales colisiones puedan ocurrir. Como el demandado argumenta, él sabe que sus automóviles pueden ser conducidos a zonas con agua, pero no se sugiere que tenga el deber de equiparlos con flotadores». Desde mi punto de vista, el problema en la argumentación del caso estuvo en la utilización del término

Automotive Engineers (SAE). Vid. NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Federal Automated Vehicles Policy Accelerating the Next Revolution in Roadway Safety*, september, 2016. En España, explican dicha clasificación entre otros, LÓPEZ MAS, P. J., *Óp. Cit.*, 2024, pp. 61 y ss; LAFUENTE SÁNCHEZ, R., «Inteligencia artificial y vehículos autónomos: responsabilidad civil extracontractual internacional», *Aranzadi*, 2024, pp. 70 y ss y ELIZALDE SALAZAR, I., *Óp. Cit.*, 2022, pp. 30 y ss.

¹⁸ Respecto a los Estados que han utilizado esta doctrina Vid. SHAD, K. A., «Warren v. Colombo: North Carolina Recognizes Claim for Enhanced Injury», *North Carolina Law Review*, vol. 68, 1990. Sin embargo, existe alguna voz en la actualidad que ha afirmado que esta doctrina se ha desvirtuado o incluso que está desapareciendo. Vid. RICCI, E. M.; LEOPOLD, T. J.; y SALZILLO, B. «Minority Gets It Right: The Florida Supreme Court Reinvigorates the Crashworthiness Doctrine in D'Amario v. Ford», *Florida Bar Journal*, vol. 78, june, 2004; y ROTH, L. M. «Florida's Motor Vehicle Crashworthiness Enhanced Injury Doctrine "Wanted dead or..." », *Barry Law Review*, vol. 18, n° 2, 2013.

¹⁹ Vid. MADDEN M. S., *Óp Cit.*, 1988, p. 306; y LAWRENCE MAC DOUGALL, V., *Óp Cit.*, 1990.

²⁰ GOLDEN, R. A., «Automobile Crashworthiness - The Judiciary responds when manufacturers improperly design their cars», *Insurance Counsel Journal*, vol. 46, n° 3, july, 1979, pp. 340 y 341.

may, que introduce en la argumentación un margen de posibilidad, es decir, se trataron las colisiones como meras posibilidades en la conducción de vehículos, cuando en realidad, la existencia de colisiones es una auténtica certeza. El tribunal comparó la posibilidad de que los vehículos fuesen conducidos por el agua con la existencia de colisiones entre vehículos, cuando estadísticamente son escasamente equiparables. Y una vez identificadas las colisiones como posibilidades dentro de la circulación viaria, declaró el Tribunal que rara vez podría imponerse una responsabilidad ante una mera posibilidad, puesto que el productor no es un asegurador del producto²¹. Señaló finalmente el Tribunal que sería deseable poderle exigir a los productores de automóviles una construcción segura también ante posibles choques, pero que esto no debe ser una labor judicial, sino legislativa y que, en su caso, debería elaborarla el legislador²². De hecho, alguna sentencia posterior, que acogió la doctrina *crashworthiness*, también apuntó en esta dirección²³, afirmando que el número y complejidad de factores que subyacen en la evaluación de la capacidad de choque de un vehículo conviene que sea una función legislativa que, en su caso, se delegue a un organismo administrativo. De igual modo, existen voces para los que los jueces y jurados carecen de la capacitación o experiencia necesaria para llevar a cabo investigaciones exhaustivas y sofisticadas sobre esta materia, siendo fundamental para el desarrollo de la interpretación de la doctrina *crashworthiness* los conocimientos científicos y técnicos del momento²⁴. En opinión de estos autores son las agencias administrativas quienes poseen la experiencia, la imparcialidad y las posibilidades de investigación requeridas para establecer directrices objetivas. Por todo ello, estos au-

²¹ Vid. HOUSER, F. D., «Crashworthiness: Defective Product Design - Secondary Impact Liability in Texas», *ST. Mary's Law Journal*, vol. 4:303, 1974, p. 306; GARIBALDI, D. A., «Defenses to Products Liability Cases», *Chicago-Kent Law Review*, vol. 48, n° 1, 1971; GALLAGHER, M.R., «Preparation of the Defense of an Automobile Products Liability Case», *9 Forum* 187, 1973.

²² Como indica AL MUREDEN, E., «Autonomous cars responsabilità civile tra disciplina vigente e prospettive *de iure condendo*», *Contratto e impresa*, vol. 35, n° 3, 2019, p. 898, el legislador, de hecho, debe definir las características técnicas del vehículo así como garantizar que puede alcanzar un nivel razonable de seguridad tanto en los aspectos funcionales para evitar el propio accidente, a lo que se refiere con el nombre de seguridad activa, como en lo referente a proteger a los pasajeros en caso de colisión, lo que denomina como seguridad pasiva.

Vid. también *Campo v. Scofield*, 301 N.Y. 468, 95 N.E.2d 80 (1950), *Ford Motor Co. v. Simpson*, 233 So. 2d 797 (1970), *General Motors Corp. v. Howard*, 244 So. 2d 726 (1971) (1971), *Yetter v. Rajeski* 364 F. Supp. 105 (D.N.J. 1973) y *Ford Motor Co. v. Havlick* 351 So. 2d 1050 (Fla. Dist. Ct. App. 1977).

²³ Por ejemplo, la sentencia *Nicolodi v. Harley Davidson Motor Co., Inc.*, 370 So. 2d 68 (Fla. 2d DCA 1979).

²⁴ Entre otros O'CONNEL, J., «Taming the Automobile» *Northwestern University Law Review*, Vol. 58, n° 3, 1963; HOENIG, M.; y GOETZ, C. H., «A rational approach to crashworthy automobiles: The need judicial responsibility». *Southwestern University Law Review*, vol. 6, 1974; NOEL, D. W., «Products Defective because of inadequate Directions or Warnings», *Southwestern Law Journal*, vol. 23, 1969; Y PAWLAK R. R., «The Second Collision concept in products liability: Philosophies and Directions», 16 *For the defense* 73, 1975.

tores entienden que muchos de los problemas judiciales que puede acarrear la doctrina *crashworthiness* se solventarían incorporando a este tipo de procedimientos una fase probatoria que acogiera el estado de las normas artísticas, gubernamentales e industriales, así como testimonios científicos, minimizando la posibilidad de que un juez de primera instancia esquivе la cuestión y lo deje todo en manos del jurado. Parece contradictoria la reflexión de estos autores, pues el que determinados productos pasen exámenes administrativos para certificar que son lo suficientemente seguros para su comercialización, no significa que la mayoría de estos análisis alcancen el máximo nivel de seguridad con respecto al nivel de los conocimientos científicos y técnicos. Por otro lado, resulta coherente y razonable que sean expertos los que examinen en un proceso judicial los distintos aspectos del producto, en estos casos, un vehículo, lo que, de ninguna manera podría acarrear que los niveles de seguridad establecidos por parte del legislador, puestos en práctica en los exámenes previos a su comercialización, pudieran vincular a los tribunales, o a los expertos que fueran a informar al respectivo procedimiento judicial. Además, no debemos olvidar que la tecnología está constantemente en desarrollo, no sólo proporcionando a los productos elementos que aumentan su seguridad, sino también interviniendo en los procedimientos de prueba de prototipos, asegurando al máximo su posterior utilización²⁵, lo que, además, en supuestos de los vehículos y, más precisamente, el de los vehículos automatizados, se pone habitualmente de manifiesto.

Esta interpretación fue seguida en casos posteriores como *Schemel v. General Motors Corp.* (384 F.2d 802 (7th Cir. 1967))²⁶, *Willis v. Chrysler Corp.* (264 F. Supp. 1010 (S.D. Tex. 1967))²⁷, *Walton v. Chrysler Corp.* (229 So. 2d 568 (1969))²⁸,

²⁵ Vid. En este sentido MARCOTTE, P., «Animated Evidence-Delta 191 Crash Re-Created Trough Computer Simulations at Trial», *ABA Journal*, vol. 75, 1989.

²⁶ Se trata de un caso muy interesante, donde se une el diseño del vehículo y la velocidad máxima permitida. El supuesto trata el accidente provocado por un vehículo que circulaba a 115 millas (185 km/h aprox.) que colisionó con otro automóvil. El tribunal se dividió en la argumentación en una parte minoritaria que entendía que, si un automóvil se había diseñado con la posibilidad de circular a una velocidad superior a la permitida, cualidad en la que la empresa comercializadora enfatizaba su publicidad, los conductores serían temerariamente inclinados al mal uso del vehículo, aumentando las posibilidades de accidentes, y por lo tanto de lesiones. Sin embargo, la mayoría de la Corte acogió la doctrina de *Evans v. General Motors Corp.*, y volvió a señalar que el deber de los productores es evitar defectos ocultos y latentes, pero que no está obligado a anticiparse y proteger el mal uso de su producto por parte de los conductores.

²⁷ Sentencia que trata los daños producidos en el conductor de un vehículo que tras sufrir un accidente a alta velocidad se dividió en dos. El Tribunal argumentó que el demandado/productor no tenía el deber de diseñar un automóvil que soportase una colisión a alta velocidad y mantuviese su estructura integral.

²⁸ Donde el demandante resultó herido mientras conducía al ser golpeado por otro vehículo. El demandante fue lanzado y vapuleado hacia delante y hacia detrás contra el respaldo del asiento en repetidas ocasiones, siendo golpeado también por el volante. El Tribunal distinguió entre daños que

McClung v. Ford Motor Company (333 F. Supp. 17 (S.D.W. Va. 1971))²⁹, *Alexander v. Seaboard Air Line R. R.* (346 F. Supp. 320 (1972))³⁰, *Yetter v. Rajeski* (364 F. Supp. 105 (D.N.J. 1973))³¹, *Perez v. Ford Motors Corp.* (497 F.2d 82 (5th Cir. 1974))³² entre algunos otros. Destaca también la sentencia *Shumard v. General Motors Corp.*, (270 F. Supp. 311 (S.D. Ohio, E.D., 1967)) en la que la muerte del conductor del vehículo se produjo como consecuencia del fuego surgido tras el accidente. El Tribunal volvió a cuestionarse si el productor del vehículo tiene el deber de elaborar productos a prueba de accidentes o que sean infalibles, por lo que señaló que la exigencia de un correcto diseño de un vehículo impediría que este se incendiase con un uso normal, pero que esto no incluye la posible deflagración, o en su caso, explosión, tras un accidente. Interesante también fue el caso *Muncy v. General Motors Corporation*, (357 SW 2d 430 (Tex. Civ. App., 1962)), donde se declaró que General Motors había diseñado defectuosamente el sistema de encendido de uno de sus vehículos, al poder extraerse la llave sin que se apagase el motor. Sin embargo, el Tribunal volvió a señalar que el automóvil en este caso no era peligroso si se usaba correctamente, es decir, de la manera y para el propósito al que estaba destinado. Evidentemente, el Tribunal entendió que extraer la llave sin apagar el motor no estaba dentro del uso normal y para el que está previsto el automóvil. Resulta cuanto menos curioso que, lo que hace 50 años se conceptuó como un defecto de diseño, en la actualidad se comercialice como añadido de modernidad y confort en ciertos automóviles³³. Igualmente, interesante fue el caso *Kahn v. Chrysler Corporation* (221 F. Supp. 677 (S. D. Tex. 1963)), donde se discutieron los daños sufridos por un menor que mientras montaba en bicicleta cayó sobre las ale-

pueden surgir mientras se atiende al uso previsto del automóvil, y los daños derivados de un defecto en el automóvil pero que no contribuyeron en la causa del accidente, para finalmente declarar que el productor del automóvil no es responsable por las lesiones derivadas de un accidente cuando éste no haya sido provocado por un defecto en el automóvil.

²⁹ Que versa sobre el accidente sufrido por el demandante en su Ford Mustang del 65 que tras una colisión se golpeó contra la barra de dirección, provocándole una ceguera total y definitiva. El demandante alegó que las lesiones se habían agravado por la existencia de determinados defectos de diseño en el vehículo, en concreto, en el volante, en la barra de dirección, y por la inexistencia de cinturones. El Tribunal acabó señalando que si se estableciese un deber al demandado (productor) de evitar el agravamiento de los daños en las colisiones sus precios subirían tanto que los pobres no podrían adquirir automóviles.

³⁰ En el que el demandante reclamaba por los daños sufridos tras chocar su automóvil Volkswagen con una locomotora.

³¹ El supuesto de hecho trata la colisión entre un Volkswagen del 65 (conducido por el demandante) y un Chrysler del 64. El conductor del Volkswagen demandó a la empresa automovilística al entender que las lesiones tras la colisión se habían gravado al golpearse con el volante que estaba defectuosamente diseñado y sufrir la fractura de trece costillas.

³² Donde tras una colisión, la cabina del camión del demandante se separó del chasis, lo que provocó el agravamiento de las lesiones.

³³ Similar comentario se podría hacer en la sentencia *Brown v. Landry* 555 So. 2d 1299 (1989) aunque, esta vez, referido a los cinturones en los autobuses escolares.

rones alargados y sobresalientes de un automóvil marca Dodge. El Tribunal afirmó que no se puede exigir a Chrysler Corporation que anticipe todas las posibles formas en las que una persona puede lesionarse al caer contra un automóvil, ni debería tener el deber de proteger contra todas las posibles lesiones, ni tampoco, por lo tanto, por las sufridas por el menor. Se vuelve a recordar que el deber de los productores se extiende al uso ordinario del vehículo o incluso que podría cubrirse ciertas situaciones en las que el automóvil se usa de manera negligente, pero que, en ningún caso, el productor no tiene la obligación de diseñar un automóvil que sea seguro para que un niño ande en bicicleta por él mientras éste está estacionado.

1.2.2. *Larsen v. General Motors Corp*

La doctrina de *Evans* fue ampliamente criticada³⁴, por lo que la jurisprudencia norteamericana se fue inclinando cada vez más hacia una interpretación que hiciera responsable al productor del agravamiento de las lesiones por un diseño defectuoso ante una colisión. El caso principal fue *Larsen v. General Motors Corp.* (391 F.2d 495, 503 (8th Cir. 1968))³⁵, donde se discutieron los daños producidos por el demandante tras la colisión frontal de su Chevrolet Corvair con otro vehículo. El Tribunal analizó de nuevo la interpretación de *Evans v. General Motors Corp.* declarando que la interpretación allí efectuada sobre el «uso previsto» o la «previsibilidad» del automóvil era demasiado estrecha y poco realista. Se afirmó que la finalidad de los automóviles es su utilización y uso para viajar por las calles y carreteras y que, durante estos viajes, a menudo, los automóviles se aproximan a otros, pudiéndose provocar posibles y potenciales impactos entre ellos que, a su vez, produzcan lesiones, debiendo tener el productor la obligación de tener un cuidado razonable en el diseño, evitando someter al usuario a un riesgo irrazonable de lesión en caso de colisión³⁶. Aunque reconociendo que los productores no tienen la obligación de

³⁴ Vid. NOEL, D. W., *Manufacturer's Liability for Negligence*, 33 *Tenn. L. Rev.* 444, 1966; HOENIG, M.; y WERBER, S. J., *Óp. Cit.*, 1971 y PAWLAK, R. R., «Manufacturer's Design Liability: The Expanding Frontiers of the Law», 19 *Dr. L. J.* 143, 1970.

³⁵ Definido por HOENIG, M.; y GOETZ, C. H., *Óp. Cit.*, 1974, como la «génesis» judicial de la teoría del *crashworthiness*. Vid. también LEVENSTAM, B., y LAPP, D. J., «Plaintiff's Burden of Proving enhanced Injury in *crashworthiness* cases: a clash worthy of analysis», *DePaul Law Review*, vol. 38, 1988.

³⁶ «Estamos de acuerdo -dice la sentencia- en que, según el estado actual de la técnica, un fabricante de automóviles no tiene la obligación de diseñar un vehículo a prueba de accidentes, o que sea infalible, ni siquiera uno que flote en el agua, pero dicho fabricante tiene el deber de tener un cuidado razonable en el diseño del vehículo para evitar someter al usuario a un riesgo irrazonable de lesiones en caso de colisión».

Resultan interesantes y reseñables algunos supuestos jurisprudenciales donde se discuten si ciertos sucesos son previsibles o no. Así destaca la sentencia *Green v. Denney* 742 P.2d 639 (1987) donde el vehículo colisionó con un caballo, alegando el demandante que las colisiones con animales gran-

llevar a cabo un vehículo a prueba de choques o accidentes, o que sea infalible. Para determinar el uso del producto fue fundamental la interpretación previamente elaborada en *Spruill v. Boyle-Midway* (308 F.2d 79 (4th Cir. 1962)) en la que se declaró que el productor debe conocer el medio en el cual el producto va a ser utilizado, para adecuar el diseño del producto a su uso general y a su uso público.

Larsen v. General Motors Corp. modificó la interpretación de la previsibilidad de las colisiones con los automóviles. Si en *Evans v. General Motors Corp.* el uso previsto de un automóvil³⁷ no contemplaba su participación en colisiones de ningún tipo o lo consideraba como mera posibilidad, en *Larsen* los accidentes de circulación se entienden plenamente previsibles mientras se viaja en automóvil, siendo responsables en estos casos los productores, ya fuera por la causa o contribución de los accidentes por medio de un diseño o una construcción negligente, o porque un diseño defectuoso hubiera agravado las lesiones³⁸.

Larsen v. General Motors Corp. articuló los tres elementos centrales y esenciales de la doctrina *crashworthiness*: en primer lugar que, como hemos señala-

des eran comunes y previsibles. El demandado, por el contrario, adujo que no podía ser previsible que esta colisión produjera un impacto concentrado en el vehículo en un punto particular del vehículo, y que «lo normal» sería que los daños se distribuyeran de manera más uniforme. Sin embargo, el Tribunal consideró lo contrario, es decir, que tampoco era previsible que la colisión se repartiera uniformemente. Finalmente, el Tribunal confirmó la posibilidad de haber diseñado el vehículo de una manera más segura y razonable. También son destacables las sentencias *Farrell v. John Deere Co.*, 151 Wis. 2d 45 (1989) y *Gerow v. Mitch Crawford Holiday Motors* 987 S.W.2d 359 (1999), donde se declaró que la somnolencia del conductor también estaba dentro de la previsibilidad en la conducción.

³⁷ Vid. HOUSER, F. D., *Óp Cit.*, 1974, p. 311. Donde haciendo suyas las palabras del Juez de *Bratton v. Chrysler Motors Corp.* (1972) indica que el término «no apto para su uso previsto» hace referencia a un producto ya vendido con un defecto, que es irrazonablemente peligroso para el consumidor, constituyendo un peligro más grande que aquel previsto por un consumidor ordinario con conocimientos medios del producto en el momento en el que lo adquirió.

³⁸ «Al aceptar... que el deber de diseño y construcción de un fabricante se extiende a la producción de un producto que sea razonablemente adecuado para su uso previsto... el problema se reduce a la interpretación adecuada del «uso previsto». No debe escucharse al fabricante decir que no tiene intención de que sus productos se vean involucrados en ningún accidente cuando pueda prever fácilmente y cuando sepa que la probabilidad de que durante la vida útil de su producto esté involucrado en algún tipo de accidente que produce lesiones. La función única de un automóvil no es sólo proporcionar un medio de transporte, sino que este sea seguro o tan seguro como sea razonablemente posible bajo el estado actual de la técnica». «No existe una base racional para limitar la reparación de los daños en situaciones donde el defecto en el diseño o la fabricación fue el factor causante del accidente, sino que la lesión resultante, generalmente causada por la llamada «segunda colisión» del pasajero con la parte interior del automóvil, también es previsible. Cuando las lesiones o «la agravación de las lesiones» se deben a que el fabricante no ha utilizado un cuidado razonable para evitar someter al usuario de sus productos a un riesgo irrazonable de lesiones, deben aplicarse los principios generales de negligencia».

do, las colisiones de vehículos son inevitables y razonablemente previsibles³⁹; en segundo lugar, que los productores de automóviles tienen el deber de reducir los riesgos irrazonables de las lesiones en las posibles colisiones; y, en tercer lugar, que sólo se puede reclamar responsabilidad a los productores por aquellas lesiones que se hayan causado por la existencia de un defecto en el producto, en este caso, por aquellas lesiones que se hayan agravado como consecuencia de la primera colisión, que se produjo con independencia del citado defecto⁴⁰.

Por todo ello, el Tribunal, tras declarar que simplemente estaba aplicando los principios básicos de la negligencia de la responsabilidad por productos defectuosos a los automóviles, concluyó que el productor debía ser requerido para proporcionar un vehículo razonablemente seguro para viajar y eliminar el riesgo irrazonable ante una previsible lesión⁴¹. Remarcando, además, que la mayoría de colisiones son previsibles y estadísticamente evitables⁴².

³⁹ Vid. SHAPO, M. S., *The Law of products liability*, Salem, New Hampshire, Butterworths, USA, vol. 2, 1994, pp. 21 y ss.

⁴⁰ Vid. RICCI, E. M.; LEOPOLD, T. J.; y SALZILLO, B., *Óp. Cit.*, 2004.

⁴¹ Como curiosidad, el Tribunal añadió que para aquellos casos en los que no haya sido posible un diseño que no agrave las lesiones que se puedan producir ante una posible colisión, el productor deberá advertirlo. Confirmándose una vez más la evidente relación entre los defectos de diseño y los defectos de información, y ahora también entre estos y la doctrina del *Crashworthiness*. Aunque, una correcta información y publicidad no debe servir de parapeto ante un defecto de diseño. Vid. GOLDEN, R. A., *Óp. Cit.*, 1979, p. 345. Representativa es la sentencia *Slone v. General Motors Corp.* 249 Va. 520 (Va. 1995) donde el Tribunal aceptó la declaración del demandante referente a que el productor conocía de la debilidad del techo del vehículo y que, por lo tanto, no se podía considerar que el vuelco, y el posterior agravamiento de los daños dada dicha debilidad era imprevisible. Igualmente interesante es la sentencia *Weiner v. American Honda Motor Co.* 718 A.2d 305 (Pa. Super. Ct. 1998). El supuesto de hecho trató los daños sufridos por un conductor que tras plegar sus asientos traseros transportaba un bote de óxido nítrico a presión. Tras un choque con una barandilla, el bote se deslizó hacia delante en el respaldo del asiento del conductor quedando inmovilizado entre el asiento y el cinturón de seguridad. El Tribunal en este caso entendió que el uso de este tipo de mercancías no estaba previsto para el vehículo, por el contrario, lo previsible atendiendo al informe de los peritos era el transporte de otro tipo de objetos como maletas, comestibles, bolsas de compras, etc, y, por tanto, no se hace responsable al productor, porque el vehículo no soportaba el transporte de un bidón de mercancía industrial. Lo contrario significaría convertir al productor casi en un asegurador de la seguridad (total) del producto sin tener en cuenta el uso previsto de este y de su posible carga. Vid. También, en un sentido similar, *Bowersfield v. Suzuki Motor Corp.* 111 F. Supp. 2d 612 (E.D. Pa. 2000).

Además, se ha señalado también, que para la valoración de lo que es razonable, deberán considerarse determinados factores como la probabilidad del daño, su certeza, el tipo de vehículo de que se trate, la función a la que este se destine, el coste de reducir el riesgo, las circunstancias en las que se produce el accidente, e incluso la comparación de las medidas de seguridad del producto afectado con otras de productos similares. Todo ello supone además comparar las medidas de seguridad del producto concreto con otros productos similares. Vid. MADDEN M. S., *Óp. Cit.*, 1988, pp. 308 y ss. Y también los casos *Czarnecki v. Volkswagen of Am.* 172 Ariz. 408, 411, 837 P.2d 1143, 1146 (Ct. App. 1991), y *Alami v. Volkswagen of Am., Inc.* 766 N.E. 574, 577 (N.Y. 2002).

⁴² Algunos autores han afirmado que la doctrina *Crashworthiness*, siendo un desarrollo del *Common Law*, tiene su origen en ciertas discusiones del Congreso de los Estados Unidos. En con-

Esta doctrina fue seguida posteriormente en varios casos como *Friend v. General Motors Corp.* (118 Ga. App. 763, 165 S.E. 2d 734 (1968))⁴³, *Mickle v. Blackmon* (166 S.E.2d 173, 187 (S.C. 1969))⁴⁴, *Dyson v. General Motors Corp.* (298 F. Supp. 1064 (E.D. Pa., 1969))⁴⁵, *Grundmanis v. British Motor Corp.* (308 F. Supp. 303 (E.D. Wis. 1970))⁴⁶, *Badorek v. General Motors Corp.* (11 Cal. App. 3rd 902, 90

creto, en las intervenciones y discusiones llevadas a cabo como consecuencia de la elaboración de *The National Traffic and Motor Vehicle Safety Act* de 1966 que creaba *The National Highway Traffic Safety Administration* (NHTSA). La Comisión que protagonizó estas discusiones dejó claro que el propósito explícito de esta ley era permitir que el Gobierno federal impulsase productores de automóviles que desarrollasen y aplicasen nuevas tecnologías con el objetivo de mejorar la seguridad de los diseños en los automóviles de una manera efectiva. Las primeras normas reguladoras se promulgaron para establecer una serie de directrices con el objetivo de proteger a los pasajeros de vehículos a motor. En el marco de estas normas, se introdujeron requisitos referentes a la seguridad interior de los turismos a fin de reducir al mínimo el riesgo de lesiones que se podrían generar o agravar a los ocupantes del vehículo en caso de colisión. A medida que los vehículos se hacían más sofisticados, sus normas reguladoras fueron también ampliándose, comenzando a incluir aspectos tales como los cinturones de seguridad de los ocupantes, los *airbags*, la resistencia del techo de los vehículos, el cierre lateral de la puerta, etc. *Vid.* HOGAN, R. B., «The Crashworthiness Doctrine», *American Journal of Trial Advocacy*, vol. 18, n° 37, 1994, pp. 39 y ss; ROTH, L. M., *Óp Cit.*, 2013, pp. 391 y 392 y, SHAPO, M. S. A. *Óp. Cit.*, 1993, p. 300.

⁴³ El supuesto de hecho trataba los daños sufridos por los demandantes que viajaban en un vehículo de transporte colectivo. Durante el trayecto, el conductor perdió el control y el vehículo se golpeó con un objeto de la acera que provocó que el asiento delantero se moviera. Este movimiento supuso, a su vez, que el equipaje que se encontraba situado detrás del asiento delantero cayera y ocasionara múltiples lesiones a los pasajeros. El Tribunal que conoció el asunto, en concreto, la Corte Suprema de Georgia, declaró que el productor había confirmado que el vehículo era plenamente comerciable. Sin embargo, la Corte georgiana, atendiendo a la concreta ley aplicable, declaró responsable al productor, al entender que entra dentro de lo razonablemente previsible que la carga en el vehículo, en este caso, el equipaje, pudiera moverse aun en condiciones normales mientras se circula por carretera.

⁴⁴ Sentencia de gran interés en la que se trataron los daños padecidos por el conductor de un Ford 1949 que tras una colisión sufrió numerosas lesiones al golpearse con la palanca de cambios del automóvil; lo que le provocó daños irreparables en su médula espinal que le produjo una parálisis permanente. Era evidente, por lo tanto, que los daños se agravaron al tener el automóvil un diseño defectuoso. Sin embargo, los demandados arguyeron que el diseño no era defectuoso y que los daños se agravaron por estar la palanca de cambios excesivamente desgastada. El tribunal, efectivamente, ante las pruebas obtenidas, indicó que los daños con la palanca se produjeron por el desgaste de ésta, pero que ello había sido debido a la negligente elección del material por parte de los productores, confirmando la condena al productor.

⁴⁵ Donde el Tribunal señaló que los productores de automóviles deben proporcionar más que una simple plataforma móvil capaz de transportar pasajeros de un punto a otro, y que, en su caso, el techo del vehículo debe proporcionar más que una protección contra la lluvia. Este caso es relevante además porque, en cierta medida, se empieza a vislumbrar la doctrina del diseño alternativo razonable al determinar que existía la obligación de diseñar un techo que fuera rígido (y por lo tanto más seguro) que redujera o impidiera la peligrosidad en caso de vuelco del automóvil. Similares a este caso fueron también *Nanda v. Motor Co.* y *Bremier v. Volkswagen of America*.

⁴⁶ En la que el tribunal declara que adoptar y seguir la posición de *Evans v. General Motors Corp.* sería ignorar la realidad en la que la previsibilidad de los accidentes es obvia y de conocimiento común. Se trataba de un supuesto de hecho muy similar al del *Ford Pinto*, en el que se discutía si la ubicación del tanque de gasolina creaba un riesgo irrazonable para los ocupantes del vehículo en caso

*Cal. Rptr. 305 (1970)*⁴⁷, *Engberg v. Ford Motor Company* (205 N.W. 2d 104 (S.D. 1973))⁴⁸, *Turner v. General Motors Corp.* (514 S.W.2d 497 (Tex. Civ. App. 1974))⁴⁹, *Frericks v. General Motors* (274 Md. 288, 336 A.2d 118 (1975))⁵⁰, *Buccery v. General Motors Corp.* (60 Cal. App. 3d 533, 132 Cal. Rptr. 605 (1976))⁵¹, *Hudell v. Levin* (537 F.2d 726, 733. C.A.3, (1976))⁵² y *Ford Motor Co. V. Evancho* (327 So. 2d 201 (Fla. 1976))⁵³, *Griffin v. Kia motors Corp.* (843 So. 2d 336, 338 (Fla. 1st DCA 2003))⁵⁴.

de colisión. Mientras que no se puedan eliminar todos los riesgos ni se puede diseñar un vehículo a prueba de accidentes bajo el estado actual de la técnica, se deben seguir factores de sentido común en la elaboración de los diseños, factores estos que son o deben ser bien conocidos por el productor, y los cuales minimizarán o disminuirán los efectos perjudiciales de una posible colisión.

⁴⁷ Muy similar también al caso del *Ford Pinto*. En este caso el tanque de gasolina de un deportivo Corvette se rompió tras una colisión trasera provocando un agravamiento de las lesiones ya sufridas tras la colisión pues el tanque estalló provocando múltiples quemaduras. El Tribunal aplicó con meridiana claridad la interpretación de *Larsen v. General Motors Corp.*

⁴⁸ Versa sobre la acción de responsabilidad llevada a cabo por una señora por la muerte de su marido. La muerte se produjo tras una colisión en su vehículo, del que alegaba estar mal diseñado. En principio, el diseño del vehículo implicaba el roce del cinturón con el asiento, lo que reducía su fuerza, provocando su rotura en la colisión. El Tribunal declaró que, si el cinturón de seguridad hubiera permanecido intacto, habría habido lesiones, pero no se hubiera producido la muerte del conductor, al haberse previsto el cinturón con el propósito específico de proteger al conductor.

⁴⁹ Primera sentencia del Estado de Texas donde se condena al productor del automóvil por los defectos de diseño que agravaron las lesiones tras una colisión, y no porque dicha colisión fuera provocada por los defectos. El conductor resultó herido cuando se desvió de la carretera para evitar la colisión con un camión, salió de la carretera, y al intentar volver a ella, su vehículo volcó.

⁵⁰ Donde se resuelve la responsabilidad de los daños producidos en el conductor de un automóvil, que había sufrido un accidente en el que el vehículo volcó. Dado su diseño defectuoso, los soportes del techo colapsaron y provocaron graves lesiones en la cabeza del demandante. El Tribunal confirmó que el productor tiene que aceptar el deber de proteger al usuario de un riesgo irrazonable de lesión debido a un producto mal diseñado negligentemente.

⁵¹ En la que los daños se agravaron al haber diseñado un automóvil sin reposacabezas.

⁵² En la que se trata el accidente sufrido por el Dr. Hudell que le provocó la muerte mientras conducía su Chevrolet Nova del 70 hacia al hospital donde trabajaba. Durante el trayecto, el vehículo se quedó sin combustible, teniendo que parar en el margen externo del carril izquierdo. Estacionado el vehículo, éste fue colisionado en la parte de atrás por el vehículo conducido por el demandado, que conducía a una velocidad considerable, provocando que la cabeza de Hudell golpeará su reposacabezas fuertemente. La autopsia demostró que el resto de su cuerpo simplemente tenía lesiones leves habiéndole provocado la muerte el golpe recibido en la cabeza. Por estos hechos el tribunal planteó la aplicación de la doctrina *crashworthiness*.

⁵³ De nuevo una sentencia que versa sobre la muerte de un pasajero como consecuencia de un defecto de diseño al colisionar el vehículo, aunque dicho defecto no provocara la colisión. El fallecido viajaba en el asiento trasero del vehículo cuando este colisionó con otro vehículo que estaba estacionado, tras el golpe, el mecanismo de bloqueo del asiento delantero falló y golpeó al fallecido en la cabeza, sufriendo heridas fatales. El Tribunal declaró que el productor debía haber tenido un cuidado razonable a la hora de realizar el diseño y la fabricación del vehículo, eliminando cualquier riesgo irrazonable de lesión debido a un defectuoso diseño. Se han dado, posteriormente, algunas sentencias con grandes similitudes como *Volkswagen of America v. Young* 321 A.2d 73 (Md. 1974) y *Rutherford v. Chrysler Motors Corp.* 231 N.W.2d 413 (Mich. Ct. App. 1975).

⁵⁴ En este supuesto, Griffin (demandante) sufrió unos daños que tuvieron como resultado su cuadriplejía; discutiéndose el defecto de uno de los respaldos del vehículo de marca Kia. La contro-

Resulta clarificadora, de igual forma, la sentencia *Cooper v. General Motors Corp.* (702 So. 2d 428 (Miss. 1997)) donde se alzan voces que proclaman que obligar a los productores de automóviles a enfrentarse a responsabilidades por diseños defectuosos por el «simple» hecho de no introducir *airbags* en sus diseños podría suponer el incremento de los precios de los automóviles hasta un punto insalvable para ciertos segmentos de la población. Sin embargo, el Tribunal afirmó que «su compasión va más allá de la persona herida; se extiende a todos aquellos que trabajan para ganarse la vida y desean un producto razonablemente seguro a un precio razonable».

Esta doctrina empezó a extenderse también a otros vehículos a motor como las motocicletas. Destacan en este punto sentencias como *Nicolodi v. Harley Davidson Motor Co.* (70 So. 2d 68 (Fla. Dist. Ct. App. 1979))⁵⁵ y *Bolm v. Triumph Corp.*, (71 A.D.2d 429 (N.Y. App. Div. 1979))⁵⁶, en ambas se afirmó que la participación de una motocicleta en un accidente es igual de previsible que en el caso de los automóviles. Llegando a confirmar *Nicolodi v. Harley Davidson Motor Co.* que la previsibilidad es la «piedra angular» de la doctrina *crashworthiness*, siendo las colisiones algo verdaderamente previsible y que quedan dentro del uso previsto (razonable) de un vehículo a motor⁵⁷. De la misma manera,

versia se centró en el posible resultado de la combinación dañosa del respaldo reclinado junto con el cinturón de seguridad. El demandante afirmó que la reclinación del respaldo puso en duda la efectividad de dicho cinturón de seguridad, puesto que argumentó que fue lo que le agravó los daños, tras la colisión frontal. El vehículo estaba siendo conducido por otra persona y Griffin ocupaba el asiento del copiloto. El conductor, tras quedarse dormido, se desvió de la carretera, y tras el ruido provocado, Griffin se despertó y extendió la mano al volante, como acto reflejo, para agarrarlo, aunque en principio, no lo tocó. El vehículo finalmente colisionó con un árbol de manera frontal. El diseño defectuoso del vehículo y, en concreto, del asiento y del cinturón de seguridad, supuso la presión de este último en su cuello, provocándole la citada cuádrupleja. El productor, por su lado, argumentó contrariamente, declarando que el vehículo nunca sufrió una colisión frontal, y que por el contrario simplemente volcó cuando Griffin ya no tenía el respaldo del asiento reclinado, presionando su cabeza con el interior del techo del vehículo provocándose la cuádrupleja. Esta sentencia aplica la doctrina de *Fabre v. Marin* 623 So. 2d 1182 (Fla. 1993) (que posteriormente desarrollamos). El Tribunal incluyó en el objeto del veredicto también que el conductor se quedó dormido.

⁵⁵ El demandante *Nicolodi* perdió una pierna tras chocar su motocicleta con un camión. La reclamación tenía como principal fundamento la inexistencia de dispositivos de seguridad en la motocicleta que protegieran las piernas del conductor en caso de colisión.

⁵⁶ Donde el conductor de la motocicleta que sufrió las lesiones interpuso reclamación por los daños sufridos alegando que la motocicleta contenía un objeto en la parte delantera que, aunque no fue la causa del accidente inicial, sí conllevó el agravamiento de sus lesiones en la zona pélvica.

⁵⁷ Resulta reveladora y clarificadora la asimilación llevada a cabo por el Tribunal de *Nicolodi* afirmando que «Por ejemplo, es previsible que la fabricación de martillos provoque que algunos pulgares resulten lesionados. Sin embargo, no es una limitación de la responsabilidad del productor del martillo afirmar que su deber de cuidado se extiende sólo a resultados que son «razonablemente» previsibles». El uso del calificador «razonablemente» en este contexto proporciona un estándar incierto con el que delimitar la responsabilidad del productor. «Significativamente, la frase «razonablemente previsible» no fue utilizada por el Tribunal de Larsen». Es decir, declarar que el deber de cuidado de los productores de martillos solo se extiende a los resultados que son «razonablemente»

en *Bolm v. Triumph Corp.* se reconoció que, atendiendo a los principios generales de la negligencia, el productor es responsable de todos aquellos daños por defectos tanto desconocidos como latentes en los vehículos a motor, ya sea en la construcción o en el diseño, ya que puede preverse que en el uso razonable de éste puedan producirse impactos que causen y/o agraven lesiones.

1.2.3. *Dreisontok v. Volkswagenwerk, A. G.*

La doctrina instaurada por *Larsen v. General Motors Corp.* fue algo modificada posteriormente por *Dreisontok v. Volkswagenwerk, A. G.* (489 F.2d 1066 (4th Cir. 1974))⁵⁸. En el caso se discutía la responsabilidad sobre los daños sufridos por algunos pasajeros de un microbús Volkswagen que se estrelló contra un poste telefónico. Durante el trayecto, el conductor intentó bajar la marcha del vehículo para reducir la velocidad, pero se encontró con alguna dificultad para localizar la palanca de cambios, lo que supuso que apartara los ojos del camino, moviera el volante y se desviase de la calzada chocando con el poste telefónico. Como consecuencia de ello, la pierna del demandante quedó atrapada tras el asiento y el tablero de instrumentos, sufriendo lesiones en el fémur y en el tobillo. El Tribunal declaró que, en realidad, la importancia de la doctrina de *Larsen v. General Motors Corp.* no es la previsibilidad de la colisión, respecto de la que el demandado intentó argumentar la exclusión de su responsabilidad, sino que debía recaer en el riesgo irrazonable de lesión ante la existencia de una colisión. Para el Tribunal es fundamental una actuación negligente para determinar si existe o no responsabilidad, debiendo tener en cuenta, a su vez, la probabilidad y la gravedad del daño producido, siendo primordial la finalidad y el uso previsto del vehículo⁵⁹. En definitiva, de acuerdo con *Dreisontok v. Volkswagenwerk, A. G.* cada caso implica el estudio de muchos factores a la hora de determinar si el productor ha sido lo necesariamente diligente con el diseño del vehículo, no provocando un riesgo irrazonable de lesión a los ocupantes dentro del rango de su «uso previsto». Aplicando esta interpretación, el Tribunal consideró que el demandado había actuado diligentemente en el diseño de su vehículo, puesto que este había sido descrito como «vehículo polivalente tipo furgoneta», y

previsibles no significa una limitación de su responsabilidad puesto que las lesiones en el pulgar son, efectivamente, «razonablemente previsibles». Vid. también GREEN, L., Forseeability in Negligence Law, 61 Column L. Rev. 1401, 1961.

⁵⁸ Aunque algunos autores la han considerado seguidora de *Evans v. General Motors Corp.* Vid. Por ejemplo, GALERSTEIN G., *Óp. Cit.*, 1979, p. 191.

⁵⁹ Incluso el Tribunal de *Dreisontok v. Volkswagenwerk, A. G.* llegó a señalar que el mero hecho de que las colisiones de automóviles sean lo suficientemente frecuentes como para ser previsibles no es suficiente por sí mismo como para crear una obligación por parte del productor de diseñar el automóvil para resistir dichas colisiones en cualquier circunstancia. Vid. HOENIG, M., y WERBER, S. J., *Óp. Cit.*, 1971, pp. 578 y ss.

fue diseñado con el objetivo de proporcionar el máximo espacio de carga y de pasajeros a un precio económico, aunque fuera de las dimensiones que hacen posible una maniobrabilidad sencilla⁶⁰.

1.3. APLICACIÓN DE LA DOCTRINA *CRASHWORTHINESS*. RELACIÓN DE LA PRIMERA COLISIÓN CON LA *SECOND COLLISION*: INTERVENCIÓN DE TERCERO Y CULPA DEL PERJUDICADO

1.3.1. La relevancia de las circunstancias de la primera colisión

La principal controversia en la aplicación de la doctrina *crashworthiness* se centra en el tratamiento del primer accidente o colisión, problemática que se mantendrá en los supuestos de vehículos automatizados. Debe dilucidarse si la parte que la causó también puede tener algo de responsabilidad en el aumento de las lesiones por la segunda colisión, sea un productor del *software* diferente al del vehículo en su conjunto, o simplemente un tercero. A este respecto surgieron dos líneas contradictorias de pensamiento en la doctrina *crashworthiness* clásica⁶¹. La opinión que se ha presentado como mayoritaria y que a su vez se divide en dos doctrinas distintas, y la doctrina minoritaria.

1.3.2. La doctrina mayoritaria

En primer lugar, se agrupan aquellos que entienden que a la doctrina *crashworthiness* se le deben aplicar los principios tradicionales de la responsabilidad civil, y con estos, una comparación de las culpas. La sentencia *Meekins v. Ford Motor Co.* (699 A.2d 339 (Del. Super. Ct. 1997)) es ejemplo de ello. En este caso, el demandante estando parado y, supuestamente, con la debida señalización, fue embestido por otro vehículo. Dicha colisión supuso la activación del *airbag* y el aplastamiento de sus dedos al tenerlos cerca. La reclamación del demandante únicamente se centró en la responsabilidad por los daños que había sufrido en sus dedos. Frente a ello, Ford señaló que su responsabilidad debería verse reducida por los acontecimientos que provocaron la primera colisión, alegando que en los casos de *crashworthiness*, la causa de la primera

⁶⁰ Vid. GALERSTEIN, G., *Óp. Cit.*, 1979, p. 193.

⁶¹ SHAPO, M. S. A., *Óp. Cit.*, 2017, pp. 95 y 96 indica que el propio hecho de que la esencia del *crashworthiness* implique una segunda colisión puede generar una disputa conceptual referente a la causa de las lesiones. Sin embargo, el autor, citando la sentencia *Warren v. Colombo* 377 S.E.2d 249 (1989) señaló que no había motivos que excluyeran la existencia de más de una causa en la producción de la lesión inicial y el agravamiento de estas.

colisión es necesariamente una causa próxima a la segunda colisión y, por lo tanto, a las lesiones que se han visto agravadas⁶².

También es representativa la sentencia *Hinkamp v. American Motors Corp.* (735 F. Supp. 176 (E.D.N.C. 1989)). Se centró el caso en los daños que sufrió el conductor, que patinó en una carretera con hielo sufriendo un terrible accidente que le provocó lesiones graves y permanentes. El Tribunal tuvo claro que el autor de los daños iniciales, y que tomó parte en la causa de la primera colisión, puede ser considerado responsable también de la negligencia del segundo autor de daños, es decir, del productor, ya que las lesiones que se vieron aumentadas por la segunda colisión no dejaban de ser consecuencia de la primera. De una manera similar se resolvió el caso *General Motors corp. v. Farnsworth* (965 P2d 1209 (Alaska 1998)), que trataba los daños sufridos por un conductor, que tras una primera colisión, se agravaron al tener un defecto el cinturón de seguridad. El Tribunal entendió que el responsable de la primera colisión debe considerarse causante inmediato de las lesiones causadas por una negligencia posterior, en este caso por un producto defectuoso.

La segunda corriente de pensamiento, dentro de este grupo mayoritario entiende que, en aplicación del principio de equidad, en aquellos supuestos en los que el dañado haya actuado negligentemente en la primera colisión, se podrá tener en cuenta dicho comportamiento con el objetivo de distribuir la culpa en aquellos casos en los que una segunda colisión aumente los daños. Aunque es cierto que *Larsen v. General Motors Corp.* (1968) estimó que no debería existir compensación de culpas entre el productor y el conductor (y causante inicial de la primera colisión), algunas sentencias entendieron que sería discriminatorio no tenerlo en cuenta. Destacan, como seguidoras de esta segunda corriente, entre otras, la sentencia *White head v. Toyota Motor Corp.* (897 S.W.2d 684 (1995)) que declaró que sería ilógica la aplicación de la compensación de culpa en la responsabilidad de productos en general, pero excluyéndolo para la aplicación de la doctrina *crashworthiness*. Siendo además importante el cumplimiento de determinadas consideraciones de política pública que impiden que pase inadvertida en la comparación de las actuaciones la posible conducción negligente del demandante. En la aplicación de la doctrina *crashworthiness*, el deber del productor de elaborar un automóvil que sea razonablemente seguro no debe diluir el deber del conductor de actuar diligentemente⁶³.

⁶² Vid. ROTH, L. M., *Óp Cit.*, 2013, p. 415.

⁶³ VICKLES, H. F., y OLDHAM, M. E., «Enhanced Injury Should Not Equal Enhanced Liability», *South Texas Law Review of the System of Products Liability Law*, vol. 36. 1995, p. 440.

1.3.3. La doctrina minoritaria: *D'Amario v. Ford Motor Co.*

Al contrario, el punto de vista minoritario es fiel a una doctrina *crashworthiness* bastante más estricta. Desde esta interpretación, se presumen las dos colisiones, por lo que es igualmente previsible tanto la colisión inicial como el empeoramiento de las lesiones como consecuencia de la existencia de un defecto de diseño. Los hechos desencadenantes del accidente son irrelevantes, considerándose que la posible negligencia que provocó la primera colisión es totalmente remota y que, de ninguna manera, puede ser considerada la causa del empeoramiento de las lesiones. Si *Larsen v. General Motors Corp.* (1968) evidenció la clara previsibilidad de los accidentes automovilísticos, los productores de automóviles tienen la obligación de, con sus diseños, minimizar los igualmente previsibles efectos nocivos de dichos choques, independientemente de cómo se haya causado el choque. La esencia de esta doctrina minoritaria es que la causa de la colisión inicial no puede ser considerada causa directa de las lesiones que se vieron aumentadas⁶⁴.

El ejemplo principal y que confirmó en los Tribunales de Florida la opinión minoritaria de la doctrina fue el caso *D'Amario v. Ford Motor Co.* (806 So. 2d 424 (Fla. 2001))⁶⁵. El demandante era uno de los pasajeros de un vehículo cuyo conductor estaba conduciendo bajo los efectos del alcohol. Durante el trayecto, el conductor perdió el control y el vehículo impactó contra un árbol. Tras el impacto se produjo una fuga de combustible, incendiándose el vehículo y, por tanto, agravándose las heridas que la primera colisión había provocado. La primera colisión viene representada por el choque del vehículo con el árbol, mientras que la segunda colisión se produjo con el estallido en llamas del vehículo.

Los abogados del productor demandado intentaron desviar la atención del jurado hacia el hecho de que el accidente inicial había sido provocado por una persona bajo los efectos del alcohol, dejando aparte el verdadero problema: la realidad defectuosa del vehículo al contener un diseño que no era seguro y que supuso el agravamiento de los daños provocados en la primera colisión.

El Tribunal estudió todas las posibilidades. Basándose conjuntamente en el *Restatement (Third) of Torts: Apportionment of Liability* y el *Restatement (Third) of*

⁶⁴ Vid. También sentencias como *Jimenez v. Chrysler Corp.* (74 F. Supp. 2d 548 (1999)), *Reed v. Chrysler Corp.* 494 N.W.2d 224 (1993) y *Mercurio v. Nissan Motor Corp.* 81 F. Supp. 2d 859 (2000).

⁶⁵ También se podría mencionar la Sentencia, igualmente del Tribunal Supremo de Florida *Nash v. General Motors Corp.* 734 So.2d 437 (Fla. 3d DCA 1999) cuyo supuesto de hecho se centra en el fallecimiento de María Nash mientras se dirigía a la iglesia en su automóvil, acompañada de sus dos hijos, al ser golpeada por otro vehículo, añadiéndose el fallo de su cinturón de seguridad, golpeándose la cabeza con un trozo de metal que separaba el parabrisas de la puerta del conductor. En ella ya podíamos vislumbrar los planteamientos que se consolidarían de manera definitiva en *D'Amario*.

Torts: Products Liability, incluyendo las dos variantes de la doctrina *crashworthiness*, centrándose incluso en la sentencia *Kidron, Inc. V. Carmona* (665 So. 2d 289 (1995)), donde se demostró la propia culpa del demandante (conductor) mientras se investigaba por el Tribunal el accidente inicial. En *Kidron* se declaró que se podía distribuir la culpa entre el demandante y el productor. La sentencia trataba un supuesto en el que el conductor había actuado de manera negligente al haberse dirigido con su vehículo hacia la parte trasera de un tractor que estaba detenido en la carretera; ello, unido al diseño defectuoso del tractor, hizo que no hubiese una discusión analítica sobre la diferencia entre la distribución de la culpa y la aplicación de *crashworthiness*. El Tribunal de *Kidron* no consideró la lesión resultante (en este caso, la muerte) como indivisible. El hecho de que se hablara de una compensación de culpas (*comparative negligence*) sólo se llevó a cabo con el fin de determinar cuál fue la causa de la lesión última (*crashworthiness*)⁶⁶, entendiendo que el jurado debía tener en cuenta tanto la posible responsabilidad del conductor ebrio, como la responsabilidad de General Motors.

A pesar de todo ello, *D'Amario* acogió la doctrina minoritaria. El Tribunal, junto a algunos autores⁶⁷, criticó el reparto distributivo entre ambos causantes argumentando que, aquellos jurados (piénsese que se trata de doctrina estadounidense) que priorizasen la mala conducta del conductor (en este caso se trataba de conducción bajo los efectos del alcohol), servirían como puerta de escape para los productores que pretendieran esquivar la aplicación de la doctrina *crashworthiness*. El Tribunal pretendió trazar una línea divisoria clara entre las circunstancias que concurrieron en la primera colisión y las posibles reclamaciones por aumento de las lesiones por la concurrencia de un defecto de diseño⁶⁸, dejando patente que el primer accidente no podía usarse para reducir la responsabilidad por el agravamiento de las lesiones. Para su argumentación comparó estos casos con aquellos supuestos de agravamiento de lesiones en los casos de negligencias médicas. Así, en estos casos, podemos distinguir, por un lado, las lesiones que fueron inicialmente causadas negligentemente y que requieren de atención médica y, por otro lado, las lesiones que se acentuaron tras una intervención médica negligente. En estos, el profesional médico no puede reducir su culpa por las lesiones que se agravaron aduciendo que no se participó en la causa de las lesiones que requirieron de intervención médica. De esta manera, en ambos casos se consideraba que el accidente o evento que da lugar a las lesiones iniciales simplemente crea la ocasión de

⁶⁶ YROTH, L. M., *Óp. Cit.*, 2013, pp. 397 y ss.

⁶⁷ BUBLICK, E. M., *Óp Cit.*, 2009, p. 712.

⁶⁸ Vid. REICHERT, R. C., «Limitations on Manufacturer liability in Second Collision Actions» *Montana Law Review*, vol. 43, 1982, que incluso es citado en la sentencia *D'Amario v. Ford Motor Co.* (2001).

que ocurra el segundo impacto. También hizo hincapié el Tribunal en el hecho de que el demandante tenga la carga de probar las lesiones y sus causas, tanto de la primera como de la segunda colisión; y que cuando el demandante no puede probar el agravamiento de los daños en la segunda colisión como consecuencia del defecto de diseño, en la mayoría de ocasiones, el causante de los daños de la primera colisión responderá de todo⁶⁹.

En definitiva, en *D'Amario* se afirmó que sólo la aplicación de esta manera de la doctrina *crashworthiness*, es decir, únicamente la consideración de la opinión minoritaria es fiel a los principios establecidos en *Larsen*. Se entiende que la posibilidad de que el productor pueda reducir su responsabilidad en una reclamación donde, en principio, sólo debería ponerse en cuestión su culpabilidad, podría permitir que se evitase la responsabilidad por la elaboración de un producto con un diseño defectuoso, socavando así la finalidad esencial de la doctrina *crashworthiness*.

Igualmente complejo es el supuesto en el que la persona ebria es la conductora del vehículo que sufre la colisión y los daños. Resulta ejemplificativa la sentencia *Giannini v. Ford Motor Co.* (616 F. Supp. 2d 219 (D. Conn. 2007))⁷⁰ donde el demandante alegó que, mientras conducía, a pesar de estar pisando el pedal de freno, este no reaccionaba; al contrario, el vehículo aceleró sin control, colisionando finalmente contra una barrera de hormigón y un poste de luz. Las lesiones se agravaron al fallar el cinturón de seguridad que, en principio, llevaba puesto. El demandado (Ford) argumentó que el demandante no había pisado el pedal de freno sino el acelerador, y que la realidad no se adecuaba a lo que se había declarado sobre el cinturón de seguridad, ya que efectivamente no lo llevaba puesto. La verdadera razón del accidente era que este había conducido bajo los efectos del alcohol. El dilema surge al plantearnos si en estos casos, o similares, se puede reclamar contra el productor en supuestos en los que un defecto de diseño agrava los daños, ya sea en un vehículo clásico o automatizado. En principio se podría volver a plantear que el productor tiene el deber de elaborar productos (en este caso vehículos) resistentes a los choques, independientemente de que los conductores hayan actuado negligentemente⁷¹. Si los riesgos creados por la conducta del demandante entran dentro del rango que justifica la protección contra el agravamiento de los daños que se puedan producir, este podrá esperar que el automóvil le proporcione protección. Para el Tribunal de *Giannini v. Ford*

⁶⁹ *Ibidem*.

⁷⁰ Se pueden mencionar algunas otras sentencias también importantes en el panorama estadounidense como *Daly v. General Motors Corp.* 20 Cal.3d 725 (1978) donde el demandante y dañado vio agravada sus lesiones por no usar el cinturón de seguridad. También *Korli v. Ford Motor Co.* 84 Cl. App. 3d 895 (1978).

⁷¹ De hecho, así lo cree BUBLICK, E. M., *Óp. Cit.*, 2009, pp. 719 y ss.

Motor Co., la propia existencia de la doctrina *crashworthiness* ya presupone que la lesiones se producirán, al considerar que el deber de proteger que recae sobre el productor ante el peligro de incrementarse los daños no es más que una consecuencia de la inevitabilidad negligente del conductor del vehículo, debiendo el productor, en todo caso, minimizar los efectos dañosos del accidente. El Tribunal declaró que un conductor que actúe negligentemente tiene derecho a la misma protección que un usuario diligente y cuidadoso frente a aquellas lesiones que define como «innecesarias». Expone el magistrado ponente que, si se permitiese a los productores, ante este tipo de casos, reducir o excluir su responsabilidad, podrían darse supuestos donde concesionarios, sabedores de la existencia de ciertos defectos de diseño en algunos de sus vehículos que pudiesen agravar las lesiones en supuestos de colisiones (en concreto habla de *airbags* que pueden no accionarse en caso de colisión), decidiesen venderlos a personas con un alcoholismo reconocido, siendo evidente que esta práctica no debería ser admitida. Para el Tribunal, las leyes que exigen una determinada seguridad a los productos también son aplicables a aquellos usuarios que actúan negligentemente: las regulaciones que ordenan a los productores de automóviles incluir *airbags* que se accionen de manera automática, tienen como fundamento minimizar las lesiones de los conductores en caso de colisión, siendo indiferente que el conductor sea diligente o no⁷².

1.3.4. Problemática probatoria y de desarrollo de la doctrina *crashworthiness*

La mayoría de los procedimientos estadounidenses señalados en los que se discutió sobre la doctrina *crashworthiness* se caracterizaban por ser comple-

⁷² Complementa el Tribunal su argumento, al igual que lo hizo *D'Amario*, con una analogía médica, al señalar que, si un médico debe proporcionar los mismos cuidados tanto a una persona que haya sido diligente como aquella que haya sufrido daños por su propia culpa o que ella misma se los haya provocado, igualmente debe ocurrir con los productores a la hora de elaborar y comercializar productos seguros.

Resulta interesante igualmente mencionar la sentencia *Passwaters v. General Motors Corp.* 454 F.2d 1270 (8th Cir. 1972), ya que es una de las primeras sentencias donde se plantea, tras una colisión, que un aspecto externo del diseño del vehículo pueda suponer el agravamiento de los daños producidos por la colisión. Se trataba de un accidente entre una motocicleta y un vehículo producido por *General Motors*. El conductor de la motocicleta (demandante) sufrió daños en la pierna y en el pie al entrar en contacto con el neumático del coche tras producirse la colisión. La cubierta del neumático contenía protuberancias y aletas que giraban al girar la rueda. El Tribunal entendió que el diseño del propio vehículo colisionante había agravado los daños al tener un defectuoso diseño. Se trataba de un supuesto distinto a los tradicionales casos de *crashworthiness*, pues no era defectuoso el vehículo en el que iba el dañado, sino que, por el contrario, los daños que podría haber provocado la colisión fueron unos, pero los defectos en el propio vehículo de la «primera colisión» supusieron un agravamiento de estos.

tamente teóricos. En muy pocos casos se planteó el Tribunal establecer una serie de pautas o principios que aclarasen cómo desarrollar los procedimientos que aplican esta teoría, ni mucho menos cómo los letrados debían probar el aumento de las lesiones por el diseño defectuoso, o la separación de esta segunda colisión con la primera e inicial. Ni siquiera se trató cómo debían actuar los jueces y los jurados en estos procedimientos⁷³. Sin embargo, estas cuestiones no son baladíes⁷⁴, puesto que para conocer si las lesiones se agravaron es necesario estudiar las circunstancias y consecuencias de la primera colisión, dado que, por su propia esencia, no habría segunda colisión sin otra previa o, en el caso que nos ocupa, no habría un agravamiento de los daños si no hubiese existido un defecto en el software, o si un tercero o el propio dañador no hubiese provocado la «primera colisión».

Sin embargo, en algunas sentencias sí se fueron vislumbrando, ciertamente, cuáles podrían ser algunos de estos criterios judiciales respecto a la carga probatoria de la doctrina *crashworthiness*. La primera sentencia donde se atisba es en *Hudell v. Levin* (537 F.2d 726 (3d Cir. 1976)) en la que se especificó que estos supuestos «requieren una presentación de prueba altamente refinada y casi siempre difícil». El Tribunal afirmó que debían ser los demandantes quienes demostrasen que el diseño elaborado y comercializado era defectuoso y, por lo tanto, evidenciar la existencia de un diseño alternativo razonable más seguro cuya utilización hubiese impedido el agravamiento de las lesiones, junto con el nexo causal entre este y los daños producidos⁷⁵; los daños que se habrían producido (si es que así ocurrió) en caso de haber optado por ese diseño alternativo más seguro; y un sistema que pudiera establecer la entidad de los daños sufridos que se atribuyen a ese defecto de diseño. De manera similar se entendió en *Caizzo v. Volkswagenwerk* (647 F.2d 241 (2d Cir. 1981))⁷⁶ donde

⁷³ Vid. HARRIS, T. V., «Enhanced Injury Theory: An Analytic Framework», *N.C. L. REV.*, 1984; Y DIPAOLA T. A., y RICCI E.M. «Evolution of the Automobile Crashworthiness Doctrine in Florida» *Florida Bar Journal*, vol. 69, 1995.

⁷⁴ CHADWICK, K. L., «Causing enhanced injuries in Crashworthiness Cases» *Syracuse Law Review*, vol. 48, 1998, pp. 1238 y ss. Y VICKLES, H. F., y OLDHAM, M. E., *Óp. Cit.*, 1995, pp. 426 y ss.

⁷⁵ La sentencia, sin embargo, tuvo un «voto particular» donde se afirmaba que con esa decisión se estaba imponiendo una carga de la prueba demasiado onerosa al demandante. El disidente entendió que tanto el causante del accidente inicial como el productor del vehículo debían ser tratados como *concurrent tortfeasors*. Por ello, señaló que el demandante sólo debería probar el nexo causal existente entre el perjuicio causado y el defecto del vehículo, y una vez demostrado, recaería sobre los demandados distinguir y separar las lesiones referentes a la primera colisión de las lesiones que se han agravado como consecuencia del defecto o *second collision*, y que en el caso hipotético de que no se pudieran distinguir, el productor demandado asumiría la responsabilidad de todos los daños. Vid. *Reed v. Chrysler Corp* (1992) Vid. HOENIG, M., «Understanding Second Collision Cases in New York: A suggested guide to the Application of Bolm», *New York Law Forum*, vol. 20, 1974; y ROTH, L. M., *Óp. Cit.*, 2013, p. 427.

⁷⁶ El supuesto de hecho se centra en el accidente sufrido por un matrimonio (demandantes) que mientras conducían su vehículo, en concreto un *Volkswagen*, fueron alcanzados por uno

también se analizó esta problemática. Se señaló igualmente que debía ser el demandante el que fuera requerido para demostrar el alcance de las lesiones agravadas y que se atribuían al diseño defectuoso, acreditando la naturaleza y alcance de las lesiones y cómo el citado defecto había aumentado las lesiones en comparación con el accidente inicial⁷⁷.

Esta línea de pensamiento fue fuertemente criticada, pues en muchos de los supuestos que se plantean, el demandante no tendrá ni los recursos ni las habilidades suficientes y necesarias para aportar las pruebas señaladas y, en muchas ocasiones, será imposible la distinción clara entre los daños⁷⁸, añadiéndose además el hecho de que, en definitiva, la prueba que se le está exigiendo al demandante no deja de ser la demostración de un hecho negativo, lo que hace que la prueba devenga imposible⁷⁹. Por ello, frente a aquella opinión, se contrapuso la doctrina ideada en *Fox v. Ford Motor Co.* (575 F.2d 774 (10th Cir. 1978))⁸⁰ y en *Mitchell v. Volkswagenwerk* 669 F.2d 1199 (8th Cir. 1982)⁸¹. La primera, bajo el argumento de lo establecido en el *Restatement (Second) of Torts Section 433* indicó que la carga probatoria recaería igualmente en los demandantes, que deberían probar el supuesto defecto que contribuyó al agravamiento de las lesiones. Una vez evidenciado, se trasladaba al productor la carga de distinguir las lesiones iniciales con las agravadas por el defecto, pero, si el productor no fuera capaz, como puede ocurrir, por ejemplo, en un caso de muerte, asumiría la responsabilidad solidariamente de la totalidad de los daños junto con el causante de la primera colisión⁸². También se planteó la

de los demandados. Sin embargo, los daños que esta primera colisión provocó fueron agravados al contener el vehículo defectos en los pestillos de las puertas que supusieron su apertura durante el accidente.

⁷⁷ VICKLES, H. F., y OLDHAM, M. E., *Óp. Cit.*, 1995, p. 440; y SHAD, K. A., *Óp. Cit.* 1990, p. 1335 y ss. *Vid.* también *Stonehocker v. General Motors Corp.* (1978).

⁷⁸ SHAPO, M. S. A., *Óp. Cit.*, 1994, pp. 9 y ss.

⁷⁹ SOLE i FELIU, J., *Óp. Cit.*, 1997, pp. 240 y 241.

⁸⁰ Donde se centró la discusión en la posible responsabilidad de los daños de Ford, al haber diseñado un vehículo con los asientos delanteros defectuosos por un error en la amortiguación de sus respaldos y en defectos en el diseño de los cinturones de los pasajeros de la parte trasera que no podían ser sujetados en caso de una colisión, lanzando al pasajero hacia el respaldo de los asientos delanteros.

⁸¹ La sentencia trata los daños sufridos por John Mitchell mientras viajaba como pasajero en un Karmann Ghia de 1965 fabricado y vendido por Volkswagen y conducido por Lee Mockenhaupt. Durante el trayecto, el vehículo salió de la carretera y chocó con un terraplén, rodando en múltiples ocasiones. Como consecuencia del accidente, Mitchell salió despedido al abrirse la puerta delantera del pasajero. Sufrió una dislocación fracturada de la columna vertebral a nivel de la segunda y tercera vértebra torácica y una avulsión de las raíces nerviosas a todos los niveles entre la sexta vértebra cervical y la primera vértebra torácica, lo que le supuso a la víctima la paraplejía, así como una discapacidad del 75-80% de su extremidad superior derecha.

⁸² Destaca la sentencia *Shipp v. General Motors Corp.* 750 F. 2d 418, 421(1985) que señaló que en el supuesto de que varias causas hayan producido un único daño, siendo cada una de ellas necesarias para la producción del daño, este podría ser atribuido a cualquiera de ellas, o a todas ellas. También

posible existencia de lesiones que fuesen indivisibles, cuya distinción sea irrealizable, como es el caso de la muerte, de los que debería resarcir en su totalidad el productor⁸³. *Mitchell v. Volkswagenwerk* 669 F.2d 1199 (8th Cir. 1982), por su parte, acogió la doctrina señalada, indicando que el demandante sólo tenía que demostrar que el defecto de diseño era un «factor sustancial»⁸⁴.

El *Restatement (Third) of Torts* se alineó con este mismo posicionamiento; y lo hizo apoyándose en el caso *McLeod v. American Motors Corp.* (723 F.2d 830 (11th Cir. 1984)). El supuesto de hecho trató el accidente de una mujer mientras conducía su AMC PACER que no consiguió evitar la colisión con un conductor ebrio. En la parte trasera del vehículo viajaba también su perro de raza gran danés. La fuerza provocada por la colisión supuso el lanzamiento del animal contra la parte trasera del asiento de la conductora, y esta, contra el volante y el parabrisas. El Tribunal entendió que la parte demandante únicamente debía demostrar que el defecto contribuyó sustancialmente a la producción de las lesiones. Tras ello, la carga se trasladaba al demandado, que debía distinguir y separar las lesiones producidas por el choque inicial de las lesiones agravadas como consecuencia del defecto de diseño. Y de igual manera que en los casos anteriores, si la distinción fuese posible, se podrían distribuir los resarcimientos, pero, si dicha diferenciación no fuese realizable, el productor respondería por el montante total de manera solidaria con el causante de la colisión. *McLeod v. American Motors Corp.* 723 F.2d 830 (11th Cir. 1984) citó y se basó en algunas sentencias anteriores. En concreto, *Washewich v. LaFave* 248 So. 2d 670 (Fla. Dist. Ct. App. 1971) donde se trataron los daños sufridos por el demandante tras salir despedido del vehículo al sufrir una primera colisión, y que es atropellado, posteriormente, por otro vehículo. El dañado demandó al causante del atropello, indicando el Tribunal, posteriormente, que las pruebas que se practicaron evidenciaron dos claros accidentes diferenciados y sucesivos, siendo el demandado únicamente responsable de los daños del segundo accidente. En este caso se indicó que el demandante tenía la carga de demostrar, en la medida de lo posible, qué lesiones fueron provocadas por cada uno de los accidentes y que, de no ser posible, se podría condenar al demandado, que en este caso no era el productor, por todos los daños sufridos. *McLeod* también fundamentó su posición mencionando el caso *Smith v. Fiat-Roosevelt* 556 F.2d 728 (5th Cir. 1977). En este

Lee v. Volkswagen of America Inc. 688 P.2d 1283 (Okla. 1984), donde el Tribunal Supremo de Oklahoma adoptó un punto de vista algo diferente, al indicar que solo si los daños fuesen verdaderamente distinguibles y divisibles, el demandante tendría la carga de la prueba de los daños: sin embargo, si los daños fueran únicos e indivisibles recaería sobre el productor la prueba de la divisibilidad de los daños. Vid. KEETON, W. P.; OWEN, D. G.; MONTGOMERY, J. E.; GREEN, G. *Óp. Cit.*, 1989, pp. 793 y ss. y *Sumnicht v. Toyota Motor Sales, USA Inc.* 360 N.W.2d 2 (Wis. 1984).

⁸³ Pensamiento que incluso algunos señalaron que ya se empezó a vislumbrar en *C.F. Hamblen, Inc. Vs. Owens* 172 So. 694 (Fla. 1937).

⁸⁴ Vid. ROTH, L. M., *Óp. Cit.*, 2013, p. 428.

caso, se trataron los daños sufridos por el conductor de un vehículo cuyo asiento, tras la primera colisión, colapsó, reclinándose hacia detrás repentinamente. El Tribunal entendió que en aquellos supuestos donde la lesión sea indivisible y, por ende, imposible el reparto, el demandante deberá poder resarcirse acudiendo a cualquiera de los causantes. También se citaba en *McLeod*, al defender la misma posición doctrinal, la sentencia *Humphreys v. General Motors Corp.* 839 F. Supp. 822 (N.D. Fla. 1993)⁸⁵.

Sin embargo, en la paradigmática sentencia *D'Amario v. Ford* se llevaron a cabo ciertas modificaciones a lo expresado anteriormente respecto a la carga de la prueba en los casos de *crashworthiness*. El Tribunal declaró que recaía sobre el demandante demostrar cuáles fueron las lesiones agravadas sufridas, comenzando las tareas probatorias desde el instante en el que se produjo la primera colisión. También se decidió que el productor sólo podría ser responsable del agravamiento de las lesiones, y no por los daños sufridos en la primera colisión. Sin embargo, la problemática nuevamente surgía cuando las lesiones sufridas son indivisibles⁸⁶ y el productor es incapaz de demostrar cuáles fueron las lesiones que se agravaron como consecuencia del defecto de diseño y, por lo tanto, cuáles son las lesiones que él debería resarcir y cuáles debería resarcir el causante de la colisión inicial. Algunos autores criticaron fuertemente la opción escogida por *D'Amario*⁸⁷, declarando que la *Section 768.81, Florida Statutes* podría haber servido de solución, ya que, bajo su aplicación, los Tribunales deberían emitir una valoración contra cada una de las partes responsables, estableciendo un porcentaje de culpa de cada una de ellas⁸⁸, entendiéndose su reforma en 2010 supresora de la doctrina mantenida en *D'Amario*.

El problema, nuevamente, vuelve a ser práctico, puesto que puede llegar a resultar muy complejo distinguir ciertos tipos de lesiones y diferenciar cuál ha sido su concreta causa. La variedad de casos puede ser inagotable y cada uno de ellos es distinto de los demás. No será lo mismo en el caso de *D'Amario*, donde la distinción es evidente: choque inicial con unos daños determina-

⁸⁵ El supuesto de hecho trata los daños sufridos por la Sra. Humphreys. Sufrió lesiones tras verse envuelta en un accidente múltiple, sin embargo, estas lesiones se agravaron al contener el respaldo de su asiento un defecto que supuso el bloqueo hacia la parte delantera.

⁸⁶ Vid. en este sentido, entre otras *Hinds v. General Motors Corp.* 988 F.2d 1039 (10th Cir. 1993) y *Colville v. Crown Equipment Corp.* 2002 Pa. Super. 301 (Pa. Super. Ct. 2002).

⁸⁷ Entre ellos, ROTH, L. M., *Óp. Cit.*, 2013.

⁸⁸ La primera *Section 768.81* se llevó a cabo en 1999. Posteriormente, en 2006, se reformó en un intento de acabar con la responsabilidad solidaria en estos casos de responsabilidad por productos, estableciendo como política pública la necesidad de determinar a los responsables con sus concretos porcentajes de culpa en la causación del daño. Ya en 2010 se declaró expresamente su aplicación concreta a los supuestos de *crashworthiness*, lo que paradójicamente podría suponer la eliminación de dicha doctrina tal y como se estableció en *Larsen v. Nissan Motor Co.*

dos y posterior explosión del vehículo con quemaduras claramente provocadas por la segunda colisión, que algunos otros supuestos donde la relación causa/efecto de ambos choques es similar y, por tanto, indiferenciable⁸⁹. Efectivamente, existirán casos donde aun con la participación de expertos físicos o biomédicos sea imposible realizar esta diferenciación. Es en estos supuestos donde verdaderamente radica el problema⁹⁰. En Florida, Estado de USA donde germinó la doctrina, el problema se agrava en este punto al haberse abolido una posible responsabilidad solidaria⁹¹. En España, la solución es bastante más sencilla: en aquellos supuestos donde las lesiones por ambas colisiones sean indiferenciables, la condena tanto al conductor del causante inicial como al productor será solidaria. De hecho, de la sentencia *D'Amario* podemos extraer cierta fundamentación al respecto, puesto que el Tribunal declaró que efectivamente existen supuestos donde el jurado es incapaz de separar los daños de las colisiones iniciales y secundarias⁹², y que, en el caso de que ello fuera así, deberá buscarse una solución en los precedentes jurisprudenciales. Así mismo, en la pionera sentencia *Larsen v. Nissan Motor Co.* se llegó a señalar que en un caso de lesión indivisible se debe intentar calcular la cantidad total del daño sufrido por el demandante y cuál ha sido el porcentaje de culpa de cada uno de los intervinientes. Añadiéndose que, cuando los

⁸⁹ Vid. HYDE. A. S., *Crash injuries: how and why they happen a primer for anyone who cares about people in cars*, Hyde Assocs., Julio, 1993. Aun así, y como señaló la sentencia *Norwest Bank N.M., N.A. v. Chrysler Corp.* 981 P.2d 1215 (N.M. App. 1999) «esta consideración de una lesión divisible y la responsabilidad por una lesión mejorada es solo si el agravio sucesivo, es decir, el defecto de *crashworthiness*, se establece como una causa inmediata de lesión mejorada», o sea, que la consideración de que una lesión es indivisible, y la responsabilidad por haberse agravado los daños es solo posible si el agravio sucesivo, el que efectivamente provoca la aplicación de la doctrina *crashworthiness*, se establece como una causa inmediata de la lesión mejorada.

⁹⁰ De hecho, se ha llegado a señalar que estos no son casos concretos de *crashworthiness*, sino supuestos de concurrencia de culpas. Vid. ROTH, L. M. *Óp. Cit.*, 2013.

⁹¹ Para ROTH, L. M., *Óp. Cit.*, 2013, pp. 399 y 421 y ss, la conclusión resulta de interés. El autor idea un nuevo modo de determinar cuándo un producto tiene un defecto en aquellos supuestos de aplicación de la doctrina *crashworthiness*. Destaca que un automóvil tendrá defectos de diseño o fabricación cuando se haya creado un entorno irrazonablemente peligroso para la protección del ocupante una vez que el vehículo esté involucrado en un accidente o un impacto. Una vez determinada dicha existencia, se deberá indagar en cuestiones tales como si fue la velocidad del primer accidente un factor causal de la lesión; si el determinado dispositivo de seguridad que se cuestione (en el caso de que así sea) funcionó correctamente; si dicho dispositivo de seguridad era comparable al de vehículos a motor similares; cuál fue la gravedad del choque entre el vehículo y otro vehículo, o con el otro objeto; si vehículos similares han tenido accidentes idénticos, y en el caso de que fuera así, si el productor revisó adecuadamente las causas que lo provocaron; si los daños provocados por esos vehículos similares fueran parecidos; si ante la existencia de normativa federal de producción de vehículos a motor el productor la cumplió; si el demandante ha podido presentar un diseño alternativo más seguro y económicamente factible; entre algunas otras. Por último, el autor señala que todas estas instrucciones deben estar sujetas a la discrecionalidad judicial, basándose en la dinámica del juicio y en el expediente probatorio, ayudando al jurado a sopesar la culpa comparativa de las partes.

⁹² Vid. entre muchos *Caboni v. General Motors Corp.* 398 F.3d 357 (5th Cir. 2005).

daños no puedan distribuirse, no habrá razón para que las lesiones iniciales y las «sucesivas» se traten de manera diferente. Esto es, en el caso de que las lesiones sean indiferenciables y, por lo tanto, el grado de participación de los intervinientes en cada uno de ellos, en principio, idéntico, la condena deberá ser solidaria.

De igual forma fue relevante la sentencia *Fabre v. Marín* 623 So. 2d 1182 (Fla. 1993)⁹³ donde, pese a que no era un caso de *crashworthiness*, el Tribunal sostuvo que todos los intervinientes en el accidente y en las distintas colisiones deberían poder incluirse en el objeto del veredicto para que el jurado pueda decidir sobre ellos, determinando su posible responsabilidad. De esta manera, las partes responsables del primer accidente tenían que ser traídas al procedimiento, puesto que, si la práctica de las pruebas y evidencias demostraba su culpabilidad, debían ser incluidas en el objeto del veredicto para que el jurado decidiese sobre ellas. Ello lo hizo interpretando el término *party* como todas aquellas personas que habían contribuido al accidente «independientemente de si habían sido o podrían haber sido demandados». Si bien, es cierto que, en esta sentencia, no se señaló nada respecto a quién tenía la carga de la prueba de demostrar o refutar que el agravamiento de los daños se debió a un defecto de diseño en el vehículo⁹⁴.

En definitiva, los diseños de automóviles tienen que proporcionar una protección ante riesgos previsibles, un diseño ante riesgos que sabemos que pueden generarse, ya que el resto caería bajo el cajón de los riesgos del desarrollo. Por ello, en un procedimiento de aplicación de la doctrina *crashworthiness* se deben examinar todos los hechos. Sin embargo, los abogados y peritos de las partes tienen clara cuál es su misión. Así, el productor demandado intentará demostrar que las lesiones fueron provocadas por la primera colisión debido a la alta velocidad del vehículo y por las fuerzas cinéticas del choque, o que no tiene nada que ver con el diseño del vehículo, ya sea el *software* o el *hardware*. Por el contrario, el demandante utilizará todas sus armas en la contienda para minimizar la gravedad y las circunstancias de la primera colisión y probar que fue el diseño defectuoso del vehículo (aquí, como es de esperar, en los supuestos de vehículos automatizados, hablamos únicamente del diseño del hardware del vehículo) el que aumentó de manera considerable las

⁹³ El caso discutía los daños de la Sra. Marín cuando viajaba de pasajera en el automóvil mientras conducía su marido. Esta demandó a Eddie y Marie Fabre alegando que durante el trayecto habían cambiado negligentemente de carril provocando que el vehículo de los señores Marín se desviara hacia un guardarraíl. Los demandados alegaron que habían estado estacionados durante cuatro o cinco minutos antes de que se produjera la colisión, puesto que estaban cambiando un neumático pinchado, sosteniendo que había sido otro automóvil el que había provocado el accidente.

⁹⁴ Vid. CHADWICK, K. L., *Op Cit.*, 1998, pp. 1238 y ss.

lesiones sufridas⁹⁵. Si la distinción entre los daños producidos por cada una de las colisiones es posible, el demandante podrá reclamar a cada uno de los responsables por sus respectivos daños. Por el contrario, si la distinción de los daños no fuese posible, la mejor opción para que el dañado pueda resarcirse es la responsabilidad solidaria de ambos intervinientes.

2. SU CONEXIÓN CON EL CRITERIO DE RIESGO UTILIDAD Y EL DISEÑO ALTERNATIVO RAZONABLE: DE NUEVO CON LA RESPONSABILIDAD SUBJETIVA

Cabe plantearse, en este momento, si en la utilización de la doctrina *crashworthiness* debe atenderse a la conducta del productor. La mera referencia a la utilización de diseños alternativos razonables supone la subjetividad en la responsabilidad, es decir, se atenderá a la diligencia del productor, que podría haber hecho un diseño más seguro de una forma razonable, pero no lo hizo; como consecuencia, el producto ha provocado un daño y el productor será responsable⁹⁶. En estos casos, el funcionamiento es el mismo, aunque con la especialidad de que el diseño alternativo razonable, en principio, no habría servido para no producir los daños, sino para no agravar los producidos por la primera colisión.

De nuevo, una sentencia estadounidense puede darnos algo de luz al respecto. Se trata del caso *McGee v. Cessna Aircraft Co.* 82 Cal.App.3d 1005 (Cal. Ct. App. 1978). En ella el demandado (productor) reconoció su obligación de elaborar el vehículo (en este caso, un avión) a prueba de colisiones, sin embargo, añadió que ese deber tenía que medirse atendiendo a los principios generales de la negligencia; es decir: que, independientemente de la «etiqueta» que se ponga, la responsabilidad en estos casos será subjetiva, puesto que la prueba de ponderación entre el beneficio de reducir las lesiones frente al costo de eliminar el peligro se basa esencialmente en el concepto de negligencia. Aunque el Tribunal desoyó sus argumentos e indicó que el examen debe centrarse en el producto y no en la conducta del productor, entendemos que el argumento presentado por la parte demandada es correcto. La evaluación de responsabilidad puede ir dirigida, efectivamente, al producto, atendiendo a su utilidad, a los riesgos cuyo uso provoca, a la posibilidad de realización de un diseño alternativo y más seguro, al coste de este último, etc. Pero ello no

⁹⁵ Vid. VICKLES, H. F., y OLDHAM, M. E., *Óp Cit.*, 1995; ROBINSON, M. P., y CALCAGNIE, K. F., «Vehicle Roof Crush Persists During Rollover Crashes», *AAJ TRIAL*, 2000; MURPHY, J. J., «Proving Rollover Crashworthiness Claims», *AAJ TRIAL*, 1998; y ROTH, L. M., *Óp Cit.*, 2013, pp. 411 y ss.

⁹⁶ Vid. MARÍN SALMERÓN, A., *El defecto de diseño en los productos digitales*, Aranzadi, 2023, sobre el defecto de diseño y el criterio del diseño alternativo razonable, o riesgo vs utilidad.

quiere decir que no tenga nada que ver y se excluya la conducta del productor. Efectivamente, la elección última de diseño de un producto es, ciertamente, opción del productor, y el hecho de que haya decidido elaborar un producto de una determinada manera y no de otra, independientemente de sus argumentos, significa que hay que adentrarse en el estudio de su conducta.

De igual modo representativa es la sentencia *General Motors Corp. v. Edwards* (482 So. 2d 1176 (Ala. 1985)) al afirmar que la única prueba de daños que limitaría la responsabilidad del productor en casos de *second collision* sería probando que, independientemente del diseño que se hubiese utilizado, las lesiones se habrían producido igualmente. En el supuesto de que se demostrase que, con un diseño alternativo, los daños se hubieran eliminado totalmente o se hubieran reducido, el productor sería responsable⁹⁷.

Se plantea de nuevo que, «el productor», con el fin de evitar un riesgo irrazonable de daños para el usuario en caso de colisión, tiene la obligación de usar la diligencia razonable en el diseño de sus vehículos. Los accidentes, tanto por culpa como sin ella, son perfectamente previsibles por el productor y estadísticamente inevitables⁹⁸. Lo que supone que no existe razón alguna para que no se resarzan aquellos daños que con un diseño más seguro (es decir, un diseño alternativo razonable) no se hubiesen producido o agravado a partir de una *second collision*. Lo que es evidente, como decíamos antes, es que no se puede exigir al productor un diseño seguro frente a cualquier colisión, sino que deberá establecerse la obligación del productor de diseñar un vehículo seguro en relación con riesgos razonables de daño.

Y una vez más, al hablar de la posible introducción de diseños alternativos más seguros, aparece la diligencia exigida o exigible, y con ella, el «fantasma» de la responsabilidad subjetiva⁹⁹. Se ha señalado que la discusión relativa a este tipo de supuestos aparece en la esfera de la negligencia y, de hecho, así es en la mayoría de los casos¹⁰⁰, pero esta doctrina, igualmente, se ha aplicado a supuestos que se resuelven en el marco de una responsabilidad objetiva, y en estos casos lo determinante no es si el demandado actuó con la diligencia debida, sino si el producto era defectuoso o no. Ahora bien, desde mi punto de vista, dicha afirmación puede ser errónea, pues, si para conocer cuándo un bien o producto es defectuoso hay que estar a los criterios establecidos (que en nuestra legislación son criterios objetivos, determinantes de una res-

⁹⁷ En el mismo sentido *Farrell v. John Deere* (151 Wis. 2d 45 (1989)).

⁹⁸ Vid. SOLE i FELIU, J., *Óp Cit.* 1997, p. 236.

⁹⁹ Vid. También MARÍN SALMERÓN, A., «El defecto de diseño en la jurisprudencia española: sobre el *Risk-utility test* y el criterio del diseño alternativo razonable», *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (Coord. Ataz López, J., y Cobacho Gómez, J. A.), vol. 3, Thomson Reuters Aranzadi, 2021, pp. 105 y ss.

¹⁰⁰ SOLE i FELIU, J., *Óp Cit.*, 1997, p. 237.

ponsabilidad objetiva) no habría problema. Pero lo cierto es que tampoco los criterios que establece el art. 5 de la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos dejan claro, en muchas ocasiones, cuándo un producto es defectuoso, quedando, en la mayoría de las ocasiones todo a la discrecionalidad del juez, que suele, a menudo, inclinar la balanza en la dirección favorable a la víctima. Y mucho menos parece que estos criterios sean efectivos a la hora de determinar la existencia de un defecto de diseño, por lo que si recurrimos a aquellos otros criterios que se plantean para detectar un posible defecto de diseño (*risk-utility test*, o un criterio mixto entre este y las legítimas expectativas del consumidor) que son cercanos a la diligencia, seguiríamos en el mismo punto, que no es otro que el de la responsabilidad subjetiva. Reforzándose, una vez más, la idea de que los defectos de diseño deben separarse del resto de los defectos¹⁰¹.

3. LA DOCTRINA *CRASHWORTHINESS* EN LA JURISPRUDENCIA ESPAÑOLA

En la jurisprudencia española no suele aparecer esta doctrina con el término de *crashworthiness*¹⁰². Únicamente la STS de 13 de enero de 2015 (RJ 612/2015) utiliza esta denominación. Es la denominada «sentencia *Honeywell*» en la que se reclaman las responsabilidades derivadas del accidente de aviación sufrido el 1 de julio de 2002 en las proximidades de Überlingen/Lago Constanza (Alemania), cuando el avión Tupolev modelo TU-154M utilizado por la Compañía aérea BASHKIRIAN AIRLINES se estrelló en pleno vuelo contra la aeronave Boeing modelo B757-200 mientras era usada por la compañía DHL AIRWAYS¹⁰³. La acción ejercitada se fundamentaba en la respon-

¹⁰¹ Sobre la crítica al concepto de producto defectuoso de la Directiva 85/374/CEE y la necesidad de diferenciar el defecto de diseño del resto *vid.* MARÍN SALMERÓN, A., *Óp. Cit.*, 2021, p. 112 y ss; y, para el caso del concepto de producto defectuoso en las nuevas propuestas de directiva sobre responsabilidad por productos defectuosos MARÍN SALMERÓN, A., «Algunas reflexiones sobre las propuestas de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos», *Contratación en el entorno digital* (Coord. González Pacanowska, I., y Plana Arnaldos, M. C.), Aranzadi, 2023, pp. 391 y ss.

¹⁰² Pero existen algunas sentencias en las que, aun no hablando exactamente de esta doctrina, si parece que se conoce, e incluso que se aplica en cierta medida. *Vid.* SAP de 17 de enero de 2000 (AC 3465/2000).

¹⁰³ Ha desarrollado este supuesto BUSTOS MORENO, Y., «La irrupción de los drones (sistemas de aeronaves no tripuladas, UAS) y la responsabilidad civil: el futuro de los UAS autónomos», *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (Coord. Ataz López, J., y Cobacho Gómez, J. A.), vol. 1, Thomson Reuters Aranzadi, 2021, pp. 928 y ss, donde se pone de manifiesto la necesidad de demandar al fabricante.

sabilidad que incumbe a las entidades demandadas (*Honeywell International INC. Y Aviation Communications and surveillance systems (ACSS)*) en tanto que diseñadoras, fabricantes, vendedoras, distribuidoras y/o responsables del servicio de información, técnico y postventa de los sistemas de seguridad TCAS (*Traffic Collision Avoidance System*) con los que estaban equipados ambos aparatos siniestrados. Más allá de la dificultad del caso, en la que no entraremos, la doctrina *crashworthiness* aparece por primera vez en el acto del juicio del Juzgado de Primera Instancia de Barcelona n° 34 de 3 de marzo de 2010 (RJ 1992/2013) alegada por uno de los peritos de la demandante. Este sostiene «que no era posible, en este caso concreto, que los terceros a que se refieren las demandadas, el controlador aéreo y el piloto del Tupolev, pudieran considerarse «terceros responsables» y defendió que los únicos responsables del accidente lo fueron los fabricantes del sistema TCAS, las demandadas. Para defender esta tesis aludió al concepto de «capacidad de resistencia ante colisiones» (*Crashworthiness*), que se aplica a la responsabilidad civil de los fabricantes. Según esta teoría, los fabricantes tienen que fabricar sus productos de tal forma que prevengan los daños; en consecuencia, si se demuestra que el producto no era seguro, la responsabilidad civil será exclusiva del fabricante y no compartida con otras personas que puedan también haber sido negligentes. Explicó, para entenderlo, el caso del incendio de un hotel por parte de un incendiario, en el que únicamente se condenó al fabricante de la fibra acrílica de las alfombras del hotel que aceleró la combustión y no al incendiario ni al hotel por el mal funcionamiento de los aspersores, pues la acción anterior es la del fabricante que debía haber previsto el daño, esto es, que su fibra se utilizaría en alfombras de hoteles y que se podría incendiar, de modo que se le condenó por no fabricar el producto de forma que impidiera o redujera el daño. Aplicado al caso de autos, alegó que el sistema TCAS de las demandadas se diseñó y fabricó para evitar daños, accidentes aéreos, precisamente en previsión de la negligencia de otras personas, a saber, el controlador aéreo o los pilotos, de modo que, si no se consiguió, los fabricantes son los únicos responsables, sin consideración a las acciones del controlador aéreo ni del piloto». Sin embargo, para la juzgadora, no quedó claro esta posible aplicación y, en consecuencia, desoyó al perito. Dicha sentencia fue recurrida en apelación, dando lugar a la SAP de Barcelona de 7 de mayo de 2012 (JUR 259415/2012), en la que en ningún momento se menciona ni se habla de la posible aplicación de esta doctrina. No es hasta la STS de 13 de enero de 2015, antes citada, donde se vuelve a tratar la doctrina *crashworthiness* señalándose que «los demandantes alegan que este criterio legal queda exceptuado en el caso de responsabilidad por productos por aplicación de lo que denominan doctrina de la *crashworthiness*, conforme a la cual los productores tienen que fabricar sus productos de tal forma que prevengan los daños, incluso los causados por la conducta negligente de terceros. En consecuencia, si se demuestra que el

producto no era seguro, la responsabilidad civil será exclusiva del productor y no compartida con otras personas cuya actuación negligente haya contribuido a la producción del daño. Sin embargo, no han quedado suficientemente probados los términos en que tal doctrina está fijada en el Derecho de Arizona, puesto que las opiniones de los peritos de las partes son discordantes sobre este punto, sin que existan razones para otorgar más verosimilitud a unos respecto de otros. La falta de prueba suficiente y adecuada de esta excepción hace que deba prevalecer el criterio general expresado en la norma antes citada (A.R.S. 12-2506), esto es, la distribución proporcional de la responsabilidad entre los corresponsables conjuntos de acuerdo con su contribución a la lesión. Debe tomarse en consideración que la solución que en nuestro Derecho se adopta por el art. 8 de la Directiva 85/374/CEE y el art. 133 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido la Ley General para la Defensa de los Consumidores y Usuarios (en adelante, TRLGDCU) no es universal, y que es plausible que otros ordenamientos hayan optado por distribuir la responsabilidad en función de las respectivas contribuciones al daño causado»¹⁰⁴.

En cierta medida, parece el Tribunal Supremo caer en el error de entender que con la doctrina *crashworthiness* será el productor el que asuma la totalidad de la responsabilidad. Es cierto que procesalmente, y tal y como indica el art. 133 del TRLGDCU, la responsabilidad del productor no se reducirá, pero ello no excluye que posteriormente el productor le reclame al tercero responsable que le resarza su parte en la producción de los daños. Probablemente, la confusión del Tribunal venga provocada por los constantes vaivenes jurisprudenciales sufridos en los Tribunales estadounidenses con la doctrina *crashworthiness*.

En la causación de un accidente concurrirá con frecuencia la conducta de un tercero¹⁰⁵, el cual, en principio, deberá asumir su parte de responsabilidad, siendo en este punto en el que se aplica el art. 133 del TR. Se trata de una responsabilidad conjunta, en la que el demandante solicitará al productor la totalidad de la indemnización y que este, posteriormente, reclame, en su caso, al tercero.

¹⁰⁴ Cabe mencionar, aunque simplemente sea a modo representativo, algunos casos de aplicación de la doctrina en accidentes de aeronaves. Destaca *Eichstedt v. Cessna Aircraft Corp.* (No. 282, 029 (Nev., Washoe Dist. Ct. Aug. 29, 1977) donde se hizo responsable a los productores por no haber instalado arneses de hombro para los pasajeros de asientos traseros; *Fuller v. Capitol Skypark* No. 20364 (Cal. Super. Ct., Sacramento Div. Feb. 1973) en la que se condena al productor por el diseño defectuosos de los cinturones de seguridad; *Powell v. Brantly Helicopter Corp.* No. 6522 (Tex. Civ. App. Feb. 1974) donde el defecto recayó en el tren de aterrizaje al no tener la capacidad suficiente de absorción de energía; o el ya previamente comentado caso *Wilson v. Piper aircraft Corp.*

¹⁰⁵ Estamos hablando del supuesto típico en el que un automóvil conducido por X a velocidad superior a la legalmente permitida, cuya estructura ha sido diseñada por Y, es defectuosa al haberse podido elaborar un diseño más seguro a un coste razonable.

Por otro lado, en los casos en los que perjudicado y causante de la primera colisión se identifican en la misma persona, podría plantearse la aplicación del art. 145 del TRLGDCU, «la responsabilidad prevista en este capítulo podrá reducirse o suprimirse en función de las circunstancias del caso, si el daño causado fuera debido conjuntamente a un defecto del producto y a culpa del perjudicado o de una persona de la que éste deba responder civilmente». Hasta el pronunciamiento del Tribunal Supremo en la sentencia de 7 de noviembre de 2008 (LA LEY 169531/2008) la jurisprudencia al respecto no fue nada uniforme, siendo constante la aplicación de este art. 145 TR y, por lo tanto, aplicando la reducción o suprimiendo la responsabilidad del productor atendiendo a la culpa del perjudicado, como es el caso de la SAP de Madrid de 5 de mayo de 2005 que afirma que «cuando la conducta del perjudicado concurre causalmente (JUR 2005/163792) a la producción del daño se origina una moderación de la indemnización a satisfacer en función de la relevancia que tenga la actuación del perjudicado en la causación del daño (...)».

La sentencia del Tribunal Supremo de 7 de noviembre de 2008 (LA LEY 169531/2008) cambió (o, al menos, eso parece) la doctrina anterior. El supuesto de hecho trata los daños producidos como consecuencia de un accidente de circulación producido el 12 de mayo de 1998 por el demandante cuando conducía su vehículo marca Citroën ZX. El Juzgado de Primera Instancia dictó sentencia declarando la existencia de un defecto de fabricación o instalación en el airbag del vehículo puesto que no se accionó cuando debía y declarando la responsabilidad de Citroën al confirmarse que el hecho de que no se activara y funcionara correctamente dicho dispositivo de seguridad había supuesto un agravamiento de los daños que el demandante había padecido. Sin embargo, dicho juzgado aclara que, aun funcionando correctamente el airbag, ello no habría representado una protección total del actor, resultando el demandante igualmente dañado, pues únicamente hubiera supuesto que los daños no hubiesen tenido tanta gravedad. Se afirma en la sentencia que, o el conductor actuó de manera imprudente al circular sin el cinturón de seguridad, o con una pinza en el mismo que le privaba de parte de su efecto de sujeción. Teniendo en cuenta ambas realidades, el Tribunal aplicó una disminución del 40 % y, por tanto, el art. 145 TRLGDCU.

Frente a dicha sentencia se interpuso recurso de apelación y, frente a la sentencia que la resolvió, recurso de casación. El Tribunal Supremo, en lo que nos interesa, indicó que «(...) la función del airbag es proteger al ocupante del vehículo para el caso de que se produzca un accidente, con independencia de si éste se debe, o no, a una conducción inadecuada o negligente. La responsabilidad civil radica en el mal funcionamiento, o la falta de funcionamiento, del producto defectuoso, del airbag, llamado a la protección física del sujeto para el caso de accidente, y sólo en el caso de que la anomalía de fun-

cionamiento se debiese a la intervención del sujeto dañado, como si manipula o daña el producto o de algún modo resta su eficacia, incide en ella, o la hace desaparecer, debe minorarse o incluso suprimirse la responsabilidad civil del fabricante».

En mi opinión, la doctrina *crashworthiness*, como a continuación desarrollaré, se aplica en España por medio de la normativa de productos defectuosos, en concreto, a través de los arts. 133 y 145 del TRLGDCU (correspondientes al art. 8 de la Directiva 85/374/CEE). De esta manera, puede señalarse que desde una perspectiva procesal se ha optado por la doctrina minoritaria, pues el dañado puede reclamar única y directamente al productor por la totalidad de los daños y, posteriormente, éste reclamar al causante de la «primera colisión» o «primeros daños» su porcentaje indemnizatorio, más acorde con la doctrina mayoritaria. Y, para los supuestos en los que el causante de la primera colisión haya sido el propio dañado, por cualquier circunstancia, regirá la compensación de culpa, que es la aplicación material de la doctrina para estos supuestos.

4. LA APLICACIÓN DE LA DOCTRINA EN ESPAÑA: SU COMPATIBILIDAD CON EL REAL DECRETO LEGISLATIVO 8/2004, DE 29 DE OCTUBRE, POR EL QUE SE APRUEBA EL TEXTO REFUNDIDO DE LA LEY SOBRE RESPONSABILIDAD CIVIL Y SEGURO EN LA CIRCULACIÓN DE VEHÍCULOS A MOTOR

La teoría de la resistencia a los choques se basa en un derecho o en la imposición de una responsabilidad potencial contra un productor de vehículos al ser los accidentes automovilísticos previsibles. Un suceso razonablemente previsible es, por supuesto, un asunto algo menos que cierto. La justificación de la imposición de responsabilidad contra el productor de automóviles por la segunda colisión se fundamenta en la posible existencia de accidentes automovilísticos, es decir, en que estos son previsibles. No aceptar este resarcimiento, como ha dejado vislumbrar algún autor, permitiría incluso elaborar vehículos de cáscara de huevo¹⁰⁶.

No existe una base racional para limitar la responsabilidad a situaciones donde el defecto en el diseño o la fabricación fue el factor causal del accidente. Como tampoco, cuando el defecto ha aumentado las lesiones previas provocadas por el accidente. La sentencia *Dennis v. American Honda Motor Co.* 585

¹⁰⁶ En este sentido, HOUSER, F. D., *Óp. Cit.*, 1974, p. 307.

*So. 2d 1336 (1991)*¹⁰⁷ es clara al respecto. El Tribunal indicó que, un casco de motocicleta es un dispositivo de seguridad diseñado para proteger la cabeza del motociclista de lesiones, independientemente de quién causó el accidente. Sería totalmente incoherente permitir que el productor de un dispositivo de seguridad como un casco de motocicleta diseñe un producto defectuoso y, a continuación, permitir a dicho productor eludir la responsabilidad cuando el producto se utiliza para el uso previsto, es decir, el propósito del casco. Diferentes son, evidentemente, los casos en los que el dañado ha utilizado o manejado el vehículo de manera inapropiada o anormal, puesto que, en ellos, el productor no deberá responder, salvo que ambos tengan parte de culpa. Los productores no tienen el deber de diseñar o fabricar productos (en este caso, vehículos) que eviten absolutamente todo tipo de prácticas, pero sí deben elaborarlos y diseñarlos de manera que sean seguros para daños o colisiones que puedan ser razonablemente previsibles en el entorno en el que el vehículo será usado.

A estas alturas, el lector no debería tener duda de que, aun no tratándose del motivo de la primera colisión, no siendo el motivo del accidente inicial (aunque podría serlo), el defecto que provocó el aumento de las lesiones es un claro defecto de seguridad. Y al tratarse de un defecto de diseño, la mejor manera de atender a su carácter defectuoso puede ser la comparación entre la utilidad de su uso y los riesgos que provoca, e investigando si en el momento de elaboración del producto este se podría haber diseñado de una manera más segura, sin que provocase daños, y todo ello a un coste razonable.

En la mayoría de supuestos de *crashworthiness*, por su propia esencia, junto con los productores intervendrán otros sujetos cuya actuación detonará la primera colisión. Así descrito, como se ha señalado previamente, el uso del art. 8 de la Directiva puede resultar bastante evidente. Sin embargo, el término «conjuntamente» utilizado en este precepto para hacer referencia a los daños que ha producido la intervención unida del productor y de un tercero, ha planteado problemas para algunos autores¹⁰⁸, al considerar que ello no se da en los casos de *crashworthiness*. Entienden que los daños no se han causado «conjuntamente», certificando que ambos son separables: por un lado, unos primeros daños, imputables en exclusiva al tercero y no reclamables por la vía de la normativa de productos defectuosos, debiendo solicitarse su resarcimiento por medio de la regulación general. Y unos daños posteriores, que agravan los primeros sufridos, que se han derivado de la existencia en el ve-

¹⁰⁷ Se trataron los daños sufridos por Dennis, conductor motociclista que colisionó contra un tractor que transportaba troncos. Se discutió la culpabilidad del conductor y los defectos del casco que portaba Dennis en el momento de la colisión.

¹⁰⁸ SOLE i FELIU, J., *Óp. Cit.*, 1997, pp. 242 y ss.

hículo de un defecto, imputables al productor. Aunque se puede caer en una contradicción evidente en el texto, pues al hablar de la carga de la prueba, reconoce que es innecesario que se diferencie entre los daños que son atribuibles al productor y cuales, al tercero, dejando entrever, claramente, el uso del art. 8 de la Directiva.

Tampoco debe ignorarse que la mayoría de supuestos donde se aplica la doctrina *crashworthiness* son casos de accidentes de vehículos a motor y, para ellos, en España, rige el Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor. El apartado primero de su artículo 1 modificado por la Ley 35/2015, de 22 de septiembre, de reforma del sistema para la valoración de los daños y perjuicios causados a las personas en accidentes de circulación, expresa que «el conductor de vehículos a motor es responsable, en virtud del riesgo creado por la conducción de estos, de los daños causados a las personas o en los bienes con motivo de la circulación. En el caso de daños a las personas, de esta responsabilidad sólo quedará exonerado cuando pruebe que los daños fueron debidos a la culpa exclusiva del perjudicado o a fuerza mayor extraña a la conducción o al funcionamiento del vehículo; no se considerarán casos de fuerza mayor los defectos del vehículo ni la rotura o fallo de alguna de sus piezas o mecanismos. En el caso de daños en los bienes, el conductor responderá frente a terceros cuando resulte civilmente responsable según lo establecido en los artículos 1.902 y siguientes del Código Civil, artículos 109 y siguientes del Código Penal, y según lo dispuesto en esta Ley». No entraré a valorar ciertas discusiones que se hacen desde la publicación de este precepto, sin embargo, sí que debo expresar mis impresiones respecto a su potencial compatibilidad con la normativa de productos defectuosos y la doctrina *crashworthiness*. En primer lugar, podemos apreciar que el legislador ha utilizado el término «defecto», sin embargo, no existe acuerdo ni en la doctrina ni en la jurisprudencia de qué debe entenderse en este caso por «defecto». La sentencia del Tribunal Supremo de 14 de junio de 1995 (RJ 1997, 2888) aunque antigua, sigue pudiéndonos ilustrar en este sentido al expresar que «la doctrina científica y esta Sala han reiterado la distinción entre defectos del vehículo, como la rotura o fallo de sus piezas o mecanismos (entre los que podría incluirse el reventón de una rueda en avanzado estado de uso) y los defectos de conservación (entre los que pueden incluirse las omisiones del conductor en la revisión de neumáticos, que señala la Sala de instancia como no acreditada). La distinción es importante, porque mientras los vicios de funcionamiento derivados de la fabricación del vehículo pueden dar lugar a una responsabilidad cuasiobjetiva que sólo remotamente puede engarzarse con la voluntad del conductor en tanto condujo espontáneamente y, por tanto, asumió los vicios del vehículo, los defectos de conservación y la

omisión de la diligencia debida en ella derivan de su descuido o negligencia en la atención al vehículo, e integran, por tanto, el fondo de una responsabilidad culpable a la manera clásica». Por lo tanto, lo que resulta evidente es que ni legislador ni jurisprudencia parecen tener en mente los defectos de diseño a este respecto. En segundo lugar, vuelve a resultar esencial diferenciar la primera de la segunda colisión. La primera podrá deberse a multitud de motivos (choque frontal entre vehículos, alcance de vehículos, choque con especies cinéticas, accidente con algún objeto de la carretera, fallo en alguno de los *software* que dirige el vehículo, etc), y la segunda, que agravará los daños provocados por la primera, necesariamente se producirá por un defecto en el diseño -físico- del vehículo. De esta manera, cabría pensar que los primeros serán resarcidos respetando Real Decreto Legislativo 8/2005, mientras que para los segundos se aplicará todo lo establecido anteriormente respecto a la doctrina *crashworthiness* en el TRLGDCU. Sin embargo, será así -huelga decirlo una vez más- en los supuestos en los que pueda identificarse los daños provocados por cada una de las colisiones, pero habrá ocasiones (probablemente las que más) donde ello no sea posible. Además, a la práctica hay que añadir, de acuerdo con el art. 2 del Real Decreto legislativo 8/2005, la obligación de suscribir y mantener en vigor un contrato de seguro para aquellos vehículos a motor que tengan su estacionamiento habitual en España por lo que «el asegurador, dentro del ámbito del aseguramiento obligatorio y con cargo al seguro de suscripción obligatoria, habrá de satisfacer al perjudicado el importe de los daños sufridos en su persona y en sus bienes, así como los gastos y otros perjuicios a los que tenga derecho según establece la normativa aplicable»¹⁰⁹. Todo ello provoca que ante daños provocados por un accidente de circulación viaria los perjudicados o sus herederos acudan directamente a la compañía aseguradora, como así mismo permite el propio artículo 7 del Real Decreto Legislativo 8/2005. Ahora bien, aunque en la práctica sea así, y el asegurador deba responder en ese potencial procedimiento judicial tanto por los daños provocados por la primera colisión como por los agravados como consecuencia del defecto de diseño del vehículo, me parece posible y adecuado que dicha compañía aseguradora ejerza su facultad de repetición contra el productor por la cuantía correspondiente a esos segundos daños, siempre y cuando se demuestre la concurrencia de esos defectos. De hecho, el art. 10 d) del RDL 8/2005 así parece permitirlo. Esto no acarreará, desde mi punto de vista, ninguna problemática en aquellos casos en los que se puedan diferenciar ambos daños. Sin embargo, más dificultades suponen aquellos en

¹⁰⁹ Sobre las distintas problemáticas que puede acarrear la aparición de sistemas de IA y la contratación de seguros que cubran los daños que puedan provocar *vid.* MACANÁS VICENTE, G., *Óp. Cit.*, 2024, pp. 689 y ss.

los que no sean distinguibles. En estos casos, un resarcimiento solidario entre la compañía aseguradora y el productor no me parece nada descabellado.

5. LA APLICACIÓN DE LA DOCTRINA *CRASHWORTHINESS* CON LA NUEVA NORMATIVA DE RESPONSABILIDAD POR DAÑOS POR PRODUCTOS DEFECTUOSOS

El pasado 28 de septiembre de 2022 se publicó la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos¹¹⁰. En el momento de redacción de este trabajo no se ha producido su publicación como texto legal definitivo restando la aprobación por parte del Consejo una vez aceptado por el Parlamento Europeo en primera lectura. El último texto del que disponemos -que introduce modificaciones a la propuesta inicial- es el propio texto aprobado por el Parlamento Europeo en primera lectura, por lo que es con el que trabajaremos¹¹¹. Las Instituciones Europeas son conscientes de la eficacia e importancia en el resarcimiento de daños por productos defectuosos que ha tenido la Directiva 85/374/CEE durante todos estos años, sin embargo, requería de ciertas adaptaciones. El avance de las nuevas tecnologías -entre las que se debe destacar la inteligencia artificial- los nuevos modelos de negocio de economía circular, la internacionalización exponencial en las cadenas de suministro y, en definitiva, las características del mercado actual fundamentan esta modificación. Esta normativa será la que previsiblemente se aplique a los accidentes que puedan producirse con o entre vehículos automatizados o semiautomatizados siempre que se cumplan los requisitos para su aplicación y reparando aquellos daños que la normativa permite. Debe por tanto plantearse si la doctrina *crashworthiness* puede tener cabida también en esta nueva regulación y, por lo tanto, si puede llegar a plantearse su aplicación en los accidentes de estos nuevos productos. La tecnologización en la circulación, en principio, no va a impedir que los diseños de hardware de los vehículos no puedan agravar los daños tras una primera colisión. Aunque se prevé una reducción de los siniestros de accidentes automatizados y, aun cuando sea posible que la gravedad de los daños de dichos accidentes pueda ser inferior, transcurrirá un largo tiempo -si es que algún día se alcanza- hasta la obtención del supuesto de

¹¹⁰ COM (2022) 495 final.

¹¹¹ Resolución legislativa del Parlamento europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM (2022)0495) - C9-0322/2022 - 2022/0302(COD)).

accidentes cero¹¹². De esta manera, deben analizarse las herramientas que los conductores y pasajeros de los vehículos automatizados pueden disponer ante un aumento de las lesiones tras una colisión.

En el nuevo texto -al igual que ocurre con el art. 8 de la Directiva 85/374/CEE- el art. 13 (correspondiente al art. 12 en la primera propuesta publicada) establece que «(...) la responsabilidad de un operador económico no se reduzca o anule¹¹³ cuando los daños sean causados tanto por el carácter defectuoso de un producto como por un acto u omisión de un tercero». Se apuesta de nuevo, por tanto, por la opción minoritaria de la doctrina *crashworthiness* en lo que se refiere al inicio del proceso, pero pudiendo posteriormente el productor reclamar, siempre que sea posible, la distinción de los daños, aquellos que haya reparado y que haya provocado el tercero¹¹⁴.

Los propios pasajeros dañados, como sabemos, también pueden haber intervenido en la causación de parte o de la totalidad de la primera colisión, o simplemente no haber intervenido cuando debían. En los casos de vehículos con cierta automatización ya existen supuestos de accidentes donde la intervención o no ha tenido efecto en la primera colisión. En la mayoría de casos se circulaba sin que el conductor fuese pendiente o estuviese atento a la circulación¹¹⁵. En estos casos, el mismo art. 13, aunque en su apartado 2, afirma que «la responsabilidad del operador económico podrá reducirse o anularse cuando el daño sea causado conjuntamente por el carácter defectuoso del producto y por la culpa de la persona perjudicada o de una persona de la que la persona perjudicada sea responsable». Es cierto que el legislador continúa

¹¹² No debe olvidarse que, aunque la mayoría de accidentes de circulación derivan del comportamiento humano, existe un porcentaje de ellos ajeno a este factor. En Estados Unidos, por ejemplo, se prevé la existencia de un 6% de accidentes ajeno al factor humano. En Europa y, concretamente, España aumenta hasta a un 10 %. Vid. OBSERVATORIO NACIONAL DE SEGURIDAD VIAL. DIRECCIÓN GENERAL DE TRÁFICO «Las principales cifras de la siniestralidad vial España 2022», 2023; JOHANSSON, R., «Vision Zero - Implementing a policy for traffic safety», *Safety Science*, vol. 47, n° 6, 2009, pp. 826 y ss; y AL MUREDEN, E., «Event data recorder advanced driver assistance systems: la spinta gentile verso la mobilità del futuro», *Contratto e impresa*, vol. 38, n° 2, 2022, p. 402, al expresar que parece verosímil que del limitado número de estos “nuevos” accidentes se deban a defectos en el funcionamiento del vehículo, imperfecciones de la estructura de la carretera o comportamientos anormales de las personas.

¹¹³ Nótese que el legislador europeo incluye aquí también el verbo anular que no aparecía en la redacción inicial de la propuesta publicada en septiembre del 2022, ni tampoco en la Directiva del año 85 en lo que a la responsabilidad del tercero se refiere. Por el contrario, ambos textos si incluyeron esta expresión para el caso en el que propio perjudicado haya intervenido en la producción del daño. En mi opinión, no tiene mayor pretensión ni relevancia que equiparar ambos supuestos.

¹¹⁴ De hecho, el precepto comienza con la expresión «Sin perjuicio del Derecho nacional en materia de derechos de división de la responsabilidad o de repetición (...)».

¹¹⁵ LAFUENTE SÁNCHEZ, R., *Óp. Cit.*, 2024, pp. 70 y ss, desarrolla alguno de los casos de accidentes de vehículos automatizados que ya se han producido en algunos lugares del mundo.

utilizando la expresión «conjuntamente» que no está libre de críticas, sin embargo, seguimos entendiendo que es plenamente aplicable a los supuestos de agravación de las lesiones, aunque no se dé una efectiva causación conjunta de los daños.

Con la nueva regulación, la doctrina *crashworthiness* puede seguir aplicándose en supuestos de empeoramiento de daños tras un accidente o colisión, estén involucrados vehículos automatizados o, digamos, tradicionales. La introducción de programas informáticos o sistemas de Inteligencia Artificial no va a evitar la necesaria diferenciación de las lesiones sufridas si varios sujetos fueron los causantes. Demostrar dicha diferenciación, además, va a recaer sobre el perjudicado demandante, puesto que así se indica al regular la carga de la prueba y, porque las presunciones que el legislador europeo ha tenido a bien introducir para facilitar la prueba a la víctima del daño son del carácter defectuoso del producto y del nexo causal. En caso de imposibilidad en la distinción de los daños entre el productor y el tercero, el criterio de la solidaridad sigue pareciendo razonable, pero teniendo en cuenta que la responsabilidad del productor nunca se reducirá ni anulará frente a la víctima. En definitiva, también los productores de vehículos automatizados -nos referimos a todos los involucrados en el proceso de producción: programadores, diseñadores, fabricantes con carácter general, etc-, al igual que ha ocurrido y seguirá con los productores de vehículos no automatizados, deben idear sus productos atendiendo a diseños que impidan o reduzcan el daño ante posibles accidentes, sobre todo, atendiendo a una posible agravación de los daños.

6. BIBLIOGRAFÍA

AL MUREDEN, E.

«Autonomous cars responsabilità civile tra disciplina vigente e prospettive *de iure condendo*», *Contratto e impresa*, vol. 35, n° 3, 2019.

«Event data recorder advanced driver assistance systems: la spinta gentile verso la mobilità del futuro», *Contratto e impresa*, vol. 38, n° 2, 2022.

BUBLICK, E. M., «The Tort-proof plaintiff the drunk in the automobile, Crashworthiness claims, and the restatement (third) of torts», *Brooklyn Law Review*, n° 3, 2009.

BUSTOS MORENO, Y., «La irrupción de los drones (sistemas de aeronaves no tripuladas, UAS) y la responsabilidad civil: el futuro de los UAS autónomos», *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (Coord. Ataz López, J., y Cobacho Gómez, J. A.), vol. 1, Thomson Reuters Aranzadi, 2021.

- CHADWICK, K. L., «Causing enhanced injuries in Crashworthiness Cases» *Syracuse Law Review*, vol. 48, 1998.
- COLONNA, K., «Autonomous Cars and Tort Liability», *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 4, n° 4, 2012.
- ELIZALDE SALAZAR, I., *Vehículos autónomos. Responsabilidad civil y seguro*, Thomson Reuters Aranzadi, 2022.
- FAVARO, M.; NADER, N.; EURICH, S. O.; TRIPP, M.; VARADARAJU, N., «Examining accident reports involving autonomous vehicles», *Plos Onex*, 12 (9), 2017.
- FOLAND, W. J., «Enhanced Injury: Problems of Proof in Second Collision and Crashworthy Cases», *Washburn Law Journal*, vol. 16, 1977.
- GALLAGHER, M. R., «Preparation of the Defense of an Automobile Products Liability Case», *9 Forum* 187, 1973.
- GALERSTEIN G., «A review of Crashworthiness» *Journal of Air Law and Commerce* 45, n° 1, 1979.
- GARIBALDI, D. A., «Defenses to Products Liability Cases», *Chicago-Kent Law Review*, vol. 48, n° 1, 1971.
- GAVANOVIC, T. J., «Crashworthiness – Strict Liability Defective Design», *South Texas Law Journal*, vol. 17, 1975
- GOLDEN, R. A., «Automobile Crashworthiness – The Judiciary responds when manufacturers improperly design their cars» *Insurance Counsel Journal*, vol. 46, n° 3, july, 1979.
- GREEN, L., Foreseeability in Negligence Law, *61 Column L. Rev.* 1401, 1961.
- HARRIS, T. V., «Enhanced Injury Theory: An Analytic Framework», *N.C. L. REV.*, 1984.
- HOENIG, M., «Understanding Second Collision Cases in New York: A suggested guide to the Application of Bolm», *New York Law Forum*, vol. 20, 1974.
- HOENIG, M.; y GOETZ, C. H. «A rational approach to crashworthy automóviles: The need judicial responsibility». *Southwestern University Law Review*, vol. 6, 1974.
- HOENIG, M.; y WERBER, S. J.
«Automobile Crashworthiness: An Untenable Doctrine», *Cleveland State Law review*, vol. 20, n° 3, 1971.
«A rational approach to crashworthy automóviles: The need judicial responsibility». *Southwestern University Law Review*, vol. 6, 1974.
- HOGAN, R. B., «The Crashworthiness Doctrine», *American Journal of Trial Advocacy*, vol. 18, n° 37, 1994.
- HYDE. A. S., *Crash injuries: how and why they happen a primer for anyone who cares about people in cars*, Hyde Assocs., july, 1993.
- HOUSER, F. D., Crashworthiness: Defective Product Design – Secondary Impact Liability in Texas, *ST. Mary's Law Journal*, vol. 4:303, 1974.

- IZQUIERDO GRAU, G., «La responsabilidad del productor de vehículos autónomos en el marco de la (futura) legislación en materia de responsabilidad por daños causados por productos defectuosos», *Revista de Derecho Civil*, vol. 10, n° 2, 2023.
- JOHANSSON, R., «Vision Zero – Implementing a policy for traffic safety», *Safety Science*, vol. 47, n° 6, 2009.
- KEETON, W. P.; OWEN, D. G.; MONTGOMERY, J. E.; GREEN, G. *Products Liability and Safety. Cases and Materials*, 2nd, Westbury-New York, The Foundation Press, 1989.
- LAFUENTE SÁNCHEZ, R., «Inteligencia artificial y vehículos autónomos: responsabilidad civil extracontractual internacional», *Aranzadi*, 2024.
- LAWRENCE MACDOUGALL, V., *Products Liability Law in Oklahoma*, Austin-Texas, Butterworth Legal Publishers, 1990.
- LEVALLEY, D., «Autonomous vehicle liability. Application of common carrier liability», *Seattle University School of Law Digital Commons*, n° 36, 2013.
- LEVENSTAM, B., y LAPP, D. J., «Plaintiff's Burden of Proving enhanced Injury in crashworthiness cases: a clash worthy of analysis», *DePaul Law Review*, vol. 38, 1988.
- LÓPEZ MAS, P. J., «La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento», *Revista Crítica de Derecho Inmobiliario*, n° 801, 2024.
- MACANÁS VICENTE, G., «Mutualización de los riesgos generados por los sistemas de IA», *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial* (Coord. Álvarez Lata, N.), Aranzadi, 2024.
- MADDEN M. S., «Products Liability», *St. Paul Minn. West Publishing Co.*, 1988.
- MARCOTTE, P., «Animated Evidence-Delta 191 Crash Re-Created Trough Computer Simulations at Trial», *ABA Journal*, vol. 75, 1989.
- MARÍN SALMERÓN, A.,
«El defecto de diseño en la jurisprudencia española: sobre el *Risk-utility test* y el criterio del diseño alternativo razonable», *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (Coord. Ataz López, J., y Cobacho Gómez, J. A.), vol. 3, Thomson Reuters Aranzadi, 2021.
«Algunas reflexiones sobre las propuestas de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos», *Contratación en el entorno digital* (Coord. González Pacanowska, I., y Plana Arnaldos, M. C.), Aranzadi, 2023.
- El defecto de diseño en los productos digitales*, Aranzadi, 2023.
- NADER, R. «Automobile Design Hazards», *AM. JUR. Proof of Facts*, 1965.
- NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Federal Automated Vehicles Policy Accelerating the Next Revolution in Roadway Safety*, september, 2016.
- NOEL, D. W.,
Manufacturer's Liability for Negligence, 33 *Tenn. L. Rev.* 444, 1966.

- «Products Defective because of inadequate Directions or Warnings», *Southwestern Law Journal*, vol. 23, 1969.
- NÚÑEZ ZORRILLA, C., «La nueva directiva europea sobre responsabilidad civil por productos defectuosos y su aplicación a los vehículos totalmente automatizados o autónomos», *Revista Crítica de Derecho Inmobiliario*, n° 796, 2023.
- OBSERVATORIO NACIONAL DE SEGURIDAD VIAL. DIRECCIÓN GENERAL DE TRÁFICO «Las principales cifras de la siniestralidad vial España 2022», 2023.
- O'CONNEL, J., «Taming the Automobile» *Northwestern University Law Review*, Vol. 58, n° 3, 1963.
- ORTIZ FERNÁNDEZ, M., *La responsabilidad civil derivada de los daños causados por sistemas inteligentes y su aseguramiento*, Dykinson, 2021.
- PAWLAK R. R. «The Second Collision concept in products liability: Philosophies and Directions», *16 For the defense* 73, 1975.
- PROSSER. W. L., *Law of Torts*, 4ª ed., 1971.
- REICHERT, R. C., «Limitations on Manufacturer liability in Second Collision Actions» *Montana Law Review*, vol. 43, 1982.
- RICCI, E. M.; LEOPOLD, T. J.; y SALZILLO, B. «Minority Gets It Right: The Florida Supreme Court Reinigorates the Crashworthiness Doctrine in D'Amario v. Ford», *Florida Bar Journal*, vol. 78, june, 2004.
- ROBINSON, M. P. Y CALCAGNIE, K. F. «Vehicle Roof Crush Persists During Rollover Crashes», *AAJ TRIAL*, 2000.
- ROTH, L. M.,
- «Florida Supreme Court Needs a Second Look at Second Collision Motor Vehicle Cases», *Florida Bar Journal*, vol. 78, april, 2004.
- «Florida's Motor Vehicle Crashworthiness Enhanced Injury Doctrine Wanted dead or...», *Barry Law Review*, vol. 18, n° 2, 2013.
- SHAD, K. A. «Warren v. Colombo: North Carolina Recognizes Claim for Enhanced Injury», *North Carolina Law Review*, vol. 68, 1990.
- SHAPO, M. S. A.,
- The Law of products liability*, Salem, New Hampshire, Butterworths, USA, vol. 2, 1994.
- Shapo on the law of products liability*, Edward Elgar, 7ª edition, 2017.
- SOLE Í FELIU, J., *El Concepto de defecto del producto en la responsabilidad civil del fabricante*, Tirant lo Blanch, Valencia, 1997.
- VICKLES, H. F., y OLDHAM, M. E., «Enhanced Injury Should Not Equal Enhanced Liability», *South Texas Law Review of the System of Products Liability Law*, vol. 36, 1995.
- YEOMANS, G., «Autonomous vehicles: handing over control», *Lloyd's of London*, 2014.

El uso de algoritmos en detrimento de los principios jurídicos y económicos de la Unión Europea*

LUZ M. MARTÍNEZ VELENCOSO

*Catedrática de Derecho Civil
Universitat de València*

Sumario: 1. INTRODUCCIÓN. 2. TRANSPARENCIA ALGORÍTMICA. 2.1. Derecho de la competencia. 2.1.1. *Modelos de preferencia algorítmica de los propios servicios digitales*. 2.1.2. *Algoritmos de precios que facilitan una colusión ilegal entre empresas*. 2.2. Transparencia en la publicidad algorítmica. 3. DERECHO DE CONSUMO E INTELIGENCIA ARTIFICIAL. 3.1. Microtargeting. 3.2. Contratos algorítmicos. 4. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

En la UE empieza a ser una preocupación reciente la consecución de la denominada transparencia algorítmica. De este modo, se trata de favorecer que los consumidores puedan tomar decisiones razonables en el entorno digital. No obstante, la cuestión de la consecución de la deseada transparencia mediante la divulgación de los parámetros que sustentan las decisiones algorítmicas es una tarea extremadamente compleja, puesto que en los casos de empleo de programas informáticos altamente especializados resulta más fácil para las corporaciones emplear técnicas de manipulación cognitiva.

* El presente trabajo finalizado el 15 de septiembre de 2024 se enmarca en el Proyecto Prometeo 2023 titulado “Los datos como bien patrimonial: uso y protección en el mercado único digital” (CIPROM/2022/67)

Además, aunque la transparencia algorítmica es de enorme importancia, su impacto real en la toma de decisiones por parte de los consumidores puede no ser tan decisiva sobre todo en mercados donde el uso de algoritmos es frecuente, piénsese en las plataformas de transporte (como Uber o Cabify) donde se ofrecen precios dinámicos y los consumidores no tienen demasiada flexibilidad para optar a ofertas procedentes de empresas de la competencia.

Los esquemas legales de protección en la UE, que se encuentran en una fase inicial, se ciñen al marco institucional actualmente existente en materia de protección jurídica de los consumidores y usuarios, por un lado, y de protección de datos personales, por otro lado. El uso de algoritmos en transacciones de consumo es una cuestión global, y en ninguna de las jurisdicciones actuales parece recibir una respuesta integral. Hacia dónde evolucione el Derecho de protección de los consumidores en este sector puede convertir al Derecho de la Unión europea en un referente para otras jurisdicciones¹¹⁶.

En este trabajo actualmente se van a abordar diversas cuestiones que son objeto de preocupación en la Unión Europea. Por un lado, el asunto “Google Shopping”, que ha sido resuelto recientemente por la STJUE de 10 de septiembre de 2024, nos lleva a pensar que una empresa dominante como Google puede ser declarada responsable por diseñar sus algoritmos de modo que conduzca a un impacto dispar en una clase determinada de competidores en vez de la aplicación indiscriminada de esos algoritmos a todos sus productos y servicios.

Además, la implementación de algoritmos de fijación de precios podría estar teniendo un impacto considerable en el Derecho de la competencia. La inteligencia artificial permite que los competidores colaboren de manera más sutil, lo que plantea desafíos en términos de regulación. Por ejemplo, veremos casos de colusión entre hoteles que utilizan el mismo algoritmo de fijación de precios.

Por otro lado, la infracción por parte de los gigantes tecnológicos de la normativa de protección de datos se ha considerado como explotación de una posición dominante en el mercado. En este sentido, en el asunto “Meta Platforms” el TJUE estableció limitaciones en relación con el tratamiento de datos personales dentro del grupo Meta en el ámbito de su servicio de publicidad personalizada. Sin duda, esta decisión tiene implicaciones importantes para la privacidad de los usuarios y la competencia en el mercado digital.

El Reglamento de Mercados Digitales también promueve una mayor transparencia en los algoritmos utilizados en las subastas de publicidad en

¹¹⁶ Vid. Grochowski, M., Jablonowska, A., Lagioia, F., Sartor, G., “Algorithmic transparency and explainability for EU consumer protection: unwrapping the regulatory premises”. *Critical Analysis of Law: An International & Interdisciplinary Law Review*, 8(1), 2021, pp. 43-63 (p. 63).

tiempo real. Sin embargo, esta transparencia no tiene como destinatarios a los consumidores, sino a los usuarios profesionales.

Por último, la Comisión europea ha manifestado su preocupación acerca del poder de los algoritmos para influir subliminalmente en las decisiones de los ciudadanos. El Reglamento de Inteligencia artificial prohíbe la introducción en el mercado de sistemas de inteligencia artificial que tengan por fin manipular o engañar mediante el empleo de técnicas subliminales.

2. TRANSPARENCIA ALGORÍTMICA

2.1. DERECHO DE LA COMPETENCIA

La falta de transparencia, incluso en las relaciones con consumidores, puede ser perjudicial y caer dentro del ámbito de aplicación del Derecho de la competencia si resulta ser una práctica comercial desleal conforme a la Directiva 2005/29/CE sobre las prácticas comerciales desleales. Asimismo, puede cobrar importancia en aquellas situaciones de mercados desequilibrados donde un participante que ocupa una posición predominante desarrolle actuaciones no transparentes en perjuicio de otros participantes en el mercado o de los consumidores, especialmente en el entorno online impregnado de procesos algorítmicos de carácter opaco en la mayoría de los casos. Los proveedores dominantes (Google, “caso Google Shopping”, o Amazon con “Buy Box”¹¹⁷) se sirven de modelos de preferencia algorítmica de ciertos servicios, principalmente los propios en detrimento de los competidores.

Aunque la mencionada Directiva 2005/29 no se refiere expresamente a estas cuestiones, la Comisión europea aboga por una interpretación amplia de la misma a fin de resolver los problemas arriba referidos¹¹⁸. En opinión de la

¹¹⁷ La Comisión Europea ha convertido en legalmente vinculantes los compromisos ofrecidos por Amazon en virtud de las leyes antimonopolio de la UE. Estos compromisos abordan las preocupaciones de la Comisión sobre el uso de datos no públicos de los vendedores de la plataforma por parte de Amazon, así como un posible sesgo al otorgar a los vendedores acceso a su “Buy Box” y su programa Primer. Antitrust: Commission accepts commitments by Amazon (europa.eu).

Por otro lado, en EEUU se ha presentado una demanda colectiva ante un tribunal de Seattle por prácticas engañosas al entender que Amazon dirige búsquedas hacia artículos de mayor precio. Según se establece en la demanda, el algoritmo Buy Box de Amazon favorece engañosamente las propias ganancias de la compañía sobre el bienestar del consumidor.

¹¹⁸ Comunicación de la Comisión - Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, 29 de diciembre de 2021. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52021XC1229%2805%29>.

Comisión: “Los motores de búsqueda permiten buscar información en internet con arreglo a un algoritmo específico. Otros intermediarios, como los mercados en línea y los servicios de comparación de precios, ofrecen también la posibilidad de buscar entre los diferentes productos y proveedores accesibles a través de sus servicios. Los consumidores esperan que los resultados de las búsquedas sean «naturales» u «orgánicos» y se basen en criterios suficientemente imparciales. Sin embargo, los proveedores también incluyen en los resultados de las búsquedas publicidad de pago o mejoran la clasificación de los productos debido al pago directo o indirecto que reciben de los terceros comerciantes pertinentes.

La Directiva (UE) 2019/2161 añadió al artículo 7 de la DPCD un nuevo apartado 4 bis que establece un requisito específico de información sobre los principales parámetros que determinan la clasificación. Además, se añadió un nuevo punto 11 bis al anexo I de la DPCD, que prohíbe la publicidad no divulgada y la promoción remunerada en los resultados de las búsquedas”.

La DPCD prohíbe las prácticas comerciales desleales que afecten a los intereses económicos de los consumidores antes, durante y después de la celebración de un contrato. La citada Directiva distingue dos categorías principales de prácticas desleales: engañosa y agresiva. Resulta un elemento clave en la evaluación si el engaño o la práctica comercial agresiva “hace o es probable que haga que el consumidor medio tome una decisión que de otro modo no habría tomado”. Este concepto de consumidor medio resulta problemático en el tema que nos ocupa, ya que se dice que el consumidor medio es un agente económico racional, lo que lleva a la interpretación de que un agente económico racional no puede ser víctima de la explotación de sus sesgos cognitivos. Ello ha llevado a algunos autores a defender la necesidad de una interpretación flexible de este requisito en lo que se refiere al tema de la manipulación cognitiva de los consumidores en el mercado digital¹¹⁹.

Práctica comercial engañosa es aquella que “omita información sustancial que necesite el consumidor medio, según el contexto, para tomar una decisión sobre una transacción con el debido conocimiento de causa y que, en consecuencia, haga o pueda hacer que el consumidor medio tome una decisión sobre una transacción que de otro modo no hubiera tomado” (art. 7), incluso si la información es objetivamente correcta.

Por su parte, una práctica comercial es agresiva si “mediante el acoso, la coacción, incluido el uso de la fuerza, o la influencia indebida, la libertad de elección o conducta del consumidor medio con respecto al producto” se ve afectada (art. 8).

¹¹⁹ Cohen, J., “Bringing Down the Average: The Case for a “Less Sophisticated” Reasonableness Standard in US and EU Consumer Law”, 31 *LOY. CONSUMER L. REV.* 1, 33-36, 2019, pp. 40-44.

2.1.1. Modelos de preferencia algorítmica de los propios servicios digitales

A. Google Shopping Case

En cuanto a los antecedentes de este asunto, el mismo tiene su origen en el diseño tecnológico del servicio “Google Shopping” de modo que, al introducir términos de búsqueda relacionados con productos, tanto en la búsqueda general como a través de la “pestaña de compras”, el motor de búsqueda Google mostraba productos de diversos proveedores junto a sus precios. En la búsqueda general, estos resultados se encontraban en un área delimitada de “contenido patrocinado” por encima de los resultados reales de búsqueda en la web.

Tras una investigación que duró aproximadamente siete años, en 2017 la Comisión decidió que Google había infringido el Tratado de Funcionamiento de la UE, concretamente el art. 102 debido al diseño de este mecanismo. Concluyó que Google ostentaba una posición dominante en el mercado de los servicios de búsqueda general y en el mercado de los servicios de comparación de compras en línea. A juicio de la Comisión, esta situación le permitió un abuso de dicha posición que se produjo gracias al diseño (impulsado por algoritmos) de la oferta de “Google Shopping”, lo que provocó una disminución del tráfico hacia los servicios de comparación de precios de los competidores, así como un aumento del tráfico hacia el propio servicio de comparación de precios de Google. Esta autopreferencia se llevó a cabo de tal modo que los servicios de comparación de precios competidores seguían apareciendo en los resultados de búsqueda general a través de enlaces y fragmentos cortos del contenido de sus sitios web, pero no destacados en un recuadro en la parte superior de la búsqueda como el propio servicio de comparación de precios de Google. De hecho, se les relegaba en la clasificación de los resultados genéricos mediante la aplicación de los denominados “algoritmos de ajuste” (el llamado “algoritmo Panda”). Para el consumidor, que esperaba que una búsqueda genérica proporcionara una visualización neutral de contenido en Internet, esta auto-preferencia algorítmica no era transparente y por lo tanto, lo inducía a confiar únicamente en el servicio “Google Shopping” como la oferta más relevante y no a explorar resultados de clasificación inferior en busca de otras alternativas. Según la Comisión, esto privó a los servicios competidores de la posibilidad de atraer usuarios a su propia oferta y evitó que los consumidores europeos realmente pudieran elegir entre diferentes

servicios y beneficiarse plenamente de las ventajas de la innovación a través de la competencia¹²⁰.

Como resultado, la Comisión impuso a Google una multa de 2.420 millones de euros. No obstante, la cuestión de interés no son solamente las observaciones acerca de la auto-preferencia algorítmica, sino también el hecho de que Google tuvo que aportar información sobre el funcionamiento de los algoritmos de ajuste en el marco de la investigación llevada a cabo por la Comisión, es decir, hacer transparente la forma en la que funcionaba la clasificación para que pudiese ser evaluada por la Comisión.

Google y Alphabet interpusieron un recurso contra la decisión de la Comisión ante el Tribunal General de Justicia de la Unión Europea. Recurso que es desestimado con confirmación de la multa impuesta¹²¹. El Tribunal General reconoce el carácter contrario a la competencia de la práctica controvertida, puesto que Google favorece su propio servicio de comparación de precios sobre los servicios de la competencia, en lugar de un mejor resultado sobre otro resultado. Si bien es cierto que Google permitió posteriormente que los servicios de comparación de precios competidores mejoraran la calidad de la visualización de sus resultados figurando en sus «casillas» (“shopping units” o “boxes”) a cambio de una remuneración, el Tribunal General señala que dicho servicio dependía de que los servicios de comparación de precios cambiaran su modelo de negocio y dejaran de ser competidores directos de Google para convertirse en sus clientes.

Por lo que se refiere a los efectos de la práctica controvertida sobre la competencia, el Tribunal General recuerda que existe abuso de posición dominante cuando la empresa dominante, recurriendo a métodos distintos de los que rigen la competencia normal, obstaculiza el mantenimiento del grado de competencia en el mercado o el crecimiento de dicha competencia y se puede demostrar que su comportamiento puede restringir la competencia (apartado 518 de la Sentencia). Todas estas circunstancias se daban en el caso enjuiciado.

Google recurrió esta decisión ante el Tribunal de Justicia de la Unión Europea. El 11 de enero de 2024, la Abogada General Juliane Kokott publi-

¹²⁰ Vid. Resumen de la Decisión de la Comisión, de 27 de junio de 2017, relativa a un procedimiento en virtud del artículo 102 del Tratado de Funcionamiento de la Unión Europea y del artículo 54 del Acuerdo EEE [Asunto AT.39740 - Búsqueda de Google (Shopping)] [notificada con el número C(2017) 4444]. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018XC0112%2801%29>.

¹²¹ Sentencia del Tribunal General (Sala Novena ampliada) de 10 de noviembre de 2021. Google LLC, anteriormente Google Inc. y Alphabet, Inc. contra Comisión Europea. Asunto T-612/17. ECLI:EU:T:2021:763.

có sus conclusiones¹²². En su opinión, Google ha infringido el artículo 102 TFUE, ya que utilizó medios diferentes a los que rigen una competencia normal basada en méritos porque hizo valer el poder que tenía en el mercado ascendente de servicios de búsqueda general para promocionar su servicio de comparación de precios. Además, no sólo promovió su producto, sino que degradó los de la competencia. Y como sus rivales no controlaban el motor de búsqueda en línea, no pudieron enriquecer su presentación y tuvieron que sufrir la modificación del algoritmo que lo alimenta; modificación que no se aplicó al servicio de Google¹²³.

Recientemente el TJUE en su sentencia de 10 de septiembre de 2024 (Asunto C-48/22 P)¹²⁴ ha confirmado la multa impuesta a Google por haber abusado de su posición dominante en relación con su servicio de comparación de productos.

Según se hace constar en la Sentencia (apartado 267): “En el caso de autos, procede observar que, como se desprende, en particular, de los apartados 54 a 63 de la sentencia recurrida, el abuso identificado por la Comisión consistió en el posicionamiento y la presentación más favorables que Google reservaba, en las páginas de su motor de búsqueda general, a su comparador de productos frente a los comparadores de productos de la competencia. Así, la Comisión constató que, en la medida en que la capacidad de un comparador de productos para competir dependía del tráfico, ese comportamiento discriminatorio de Google había tenido un impacto importante en la competencia en la medida en que había permitido a esta sociedad desviar, beneficiándose de su comparador de productos, una gran proporción del tráfico anteriormente existente entre las páginas de resultados generales de Google y los comparadores de productos pertenecientes a sus competidores, sin que estos pudieran compensar esta pérdida de tráfico recurriendo a otras fuentes de tráfico, ya que una mayor inversión en fuentes alternativas no habría constituido una solución «económicamente viable»”. En consecuencia, se desestima el recurso de casación interpuesto por Google.

¹²² <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-01/cp240004es.pdf>

¹²³ Zingales, N., “Google Shopping: beware of ‘self-favouring’ in a world of algorithmic nudging”, *Competition Policy International-Europe Column*, 2018, p. 4: “This leaves us with the suspicion that a dominant undertaking such as Google could in fact be found liable for designing its algorithms in a way that leads to a disparate impact on a given class of competitors (or in the case of the implementation of the remedy, its competing comparison shopping services), despite the indiscriminate application of those algorithms to all products and services”.

¹²⁴ Disponible en <https://curia.europa.eu/juris/document/document.jsf?text=&docid=289925&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=1185850>.

B. Caso Buy Box Amazon

La “Buy Box” (caja de compra) es un recuadro que aparece en la página de detalle de un producto en Amazon, en la parte superior derecha. En ese lugar los clientes inician el proceso de compra al agregar un artículo a su carrito. Si un vendedor aparece en la caja de compra, significa que es el vendedor principal de ese concreto producto, obteniendo la mayoría de las ventas del mismo.

Amazon selecciona a los vendedores que participan en el “Buy Box” priorizando a aquellos que se anuncian en la plataforma de Amazon, a quienes se les exige que se abstengan de anunciar en sus propios sitios web esos productos por un precio inferior al precio de venta en Amazon.

Asimismo, Amazon diseña sus algoritmos en beneficio de los terceros vendedores que participan en su programa “Fulfillment By Amazon” y que pagan tarifas sustanciales por almacenamiento de inventario, embalaje, envío, devoluciones y otros servicios en su plataforma.

Como se ha mencionado anteriormente, la no aplicación de leyes antimonopolio en el sector tecnológico durante décadas ha conducido precisamente que empresas como Amazon, Meta, Google o Microsoft ocupen hoy en día una situación dominante en el mercado.

No obstante, en la actualidad, tanto en EEUU como en Reino Unido, se está produciendo un cambio de paradigma con el fin de cuestionar el inmenso poder de mercado de estas compañías tecnológicas.

En 2022, el fiscal general de California presentó una demanda ante el Tribunal Superior de este Estado alegando que Amazon violó tanto la “Cartwright Act” como la “Unfair Competition Law”. La demanda se sustentaba sobre la base de que Amazon estableció restricciones comerciales con sus vendedores que perjudicaron a los consumidores con violación de las leyes antimonopolio. Precisamente, las prácticas comerciales de Amazon con la “Buy Box”, al evitar que los vendedores ofrezcan sus productos al precio más bajo posible, tienen como efecto la creación de un “suelo de precios”. Esto significa que los precios no pueden caer más de cierto nivel, lo que puede afectar a la libre competencia y causar daños a los consumidores, sobre todo si este precio base es más alto que el que el vendedor hubiese fijado para el producto, forzando a los consumidores a pagar precios inflados artificialmente.

En la demanda también se alegaba que Amazon penaliza a los terceros vendedores que ofertan sus productos en otros sitios web a precios más bajos al evitar que aparezcan como vendedores predeterminados en la “Buy Box”. Estos quedarían incluidos en la sección “All Offers Display” debajo de la “Buy Box”, reduciéndose de modo dramático la posibilidad de vender.

Posteriormente, en febrero de 2024 y también en EEUU se presentó una demanda colectiva ante un tribunal federal de Seattle sobre la base de que el algoritmo de Amazon para seleccionar lo que exponer en su “Buy Box” generalmente crea confusión a la hora de distinguir las opciones de precio inferior y las opciones de envío rápido.

Según los demandantes, los compradores eligen las opciones de Amazon casi el 98% de las ocasiones al hacer clic en los botones “comprar ahora” o “agregar al carrito” creyendo erróneamente que Amazon ha encontrado los mejores precios.

Por otro lado, en el Reino Unido dos actuaciones en 2022 toman como referencia similares argumentaciones en relación con la “Buy Box” de Amazon¹²⁵.

En el ámbito de la Unión europea, la Comisión incoó un procedimiento en el asunto AT. 40703 para investigar las prácticas comerciales de Amazon relativas a: i) las condiciones y los criterios que gobiernan la selección de la oferta que aparece en la “Buy Box” y ii) las condiciones que deben darse para que los vendedores terceros puedan optar a “Prime” y sus ofertas queden vinculadas a la etiqueta “Prime”.

Realizada esta investigación, el 15 de junio de 2022 la Comisión adoptó un análisis preliminar en el que exponía sus inquietudes, el 20 de julio se publicó en el Diario Oficial una comunicación con los compromisos iniciales y a continuación, el 22 de noviembre de 2022 se publicaron ya los compromisos definitivos¹²⁶.

En particular, Amazon se ha comprometido a mostrar una segunda oferta competitiva en la “Buy Box” si esta segunda oferta es significativamente diferente de la inicial. Esta segunda oferta podría proceder de un vendedor diferente y podría tener un precio más bajo o una opción de entrega más rápida.

Los compromisos finales en relación con la “Buy Box” estarán vigentes en Europa durante siete años. El cumplimiento de tales medidas estará bajo la supervisión de la Comisión. En el caso de incumplimiento, la Comisión podría imponer una multa de hasta el 10% del volumen de negocio anual total de Amazon, o el pago de una penalización periódica del 5% por día del volumen de negocio diario de Amazon por cada día de incumplimiento.

¹²⁵ Una de ellas es una investigación realizada por la “Competition Markets Authority” y la otra una acción colectiva en la que Amazon se enfrenta a una demanda de £900m para compensar a diez millones de consumidores en el Reino Unido. Cfr. DeMelis, N., “The Antitrust Alphabet: Amazon, Buy Box, and Competition”, *Boston College Intellectual Property and Technology Forum*, 2024, pp. 1-27.

¹²⁶ Informe final del Consejo auditor Asuntos AT.40462- Amazon Market Place- y AT. 40703- Amazon Buy Box (2023/C87/04), Diario Oficial de la Unión Europea 9.3.2023.

2.1.2. Algoritmos de precios que facilitan una colusión ilegal entre empresas

En el pasado, los competidores en el mercado solían necesitar una comunicación explícita para coordinar sus acciones. Sin embargo, con la implementación de los nuevos sistemas de inteligencia artificial (IA) se está abriendo la puerta hacia nuevas formas “tácitas” de colusión¹²⁷.

Últimamente, las autoridades antimonopolio en EEUU han estado investigando una práctica que podría estar afectando a la competencia en el sector hotelero. Según una declaración conjunta del Departamento de Justicia (DOJ) y la Comisión Federal de Comercio (FTC) el uso de algoritmos de fijación de precios podría estar contribuyendo a una colusión ilegal entre los hoteles¹²⁸. Esta afirmación se hizo en el contexto del caso “Cornish-Adebiyi v. Caesars Entertainment Inc.”, No. 23-cv-02536 (D.N.J. May 9, 2023), presentado ante el Tribunal de Distrito de Nueva Jersey. Al parecer, los hoteles utilizaron una plataforma de algoritmo de precios llamada “Rainmaker”, siendo conscientes de que sus competidores también la estaban utilizando y eligiéndola precisamente por este motivo¹²⁹.

La cuestión no es nueva, hace algunos años la OCDE¹³⁰ publicó un documento en el que se analizan los desafíos que los algoritmos representan en relación con la aplicación de las normas de defensa de la competencia. En particular, se aborda la cuestión acerca de si las agencias antimonopolio deberían revisar los conceptos tradicionales de acuerdo y colusión tácita con fines antimonopolio, y discute cómo las herramientas antimonopolio tradicionales podrían utilizarse para poner fin a algunas formas de colusión algorítmica. En esta misma línea se puede consultar el informe de la CMA (“Competition and Markets Authority”) británica¹³¹. También en Europa la Autoridad Francesa de la Competencia (“French Autorité de la concurrence”) y la Oficina General de la Competencia en Alemania (“German Bundeskartellamt”) publicaron su

¹²⁷ Azzutti, A., “AI trading and the limits of EU law enforcement in deterring market manipulation”, *Computer Law & Security Review*, 45, 2022, p. 6.

¹²⁸ Se puede consultar el documento en <https://www.justice.gov/d9/2024-04/420931.pdf>.

¹²⁹ Vinod, B., “What is the future of competitive revenue management in the travel industry? *Journal of Revenue and Pricing Management*”, 2024, 1-3. También Marty, F., “Les collusions algorithmiques: mythe ou réalité?”, Sciences PO OFCE working paper, n. 9, 2024.

¹³⁰ Algorithms and collusion: Competition policy in the digital age, 14 septiembre 2017. Disponible en <https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm>.

¹³¹ De 8 de octubre de 2018. Se puede consultar en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf.

estudio conjunto sobre competencia y algoritmos¹³². En España en 2021 la CNMC impuso una multa de 1,25 millones a varias empresas por aplicar comisiones mínimas en el mercado de la intermediación inmobiliaria. En este caso, el desarrollo del software sirvió para limitar la competencia entre las inmobiliarias al establecer comisiones mínimas y otras condiciones comerciales y generar un nivel de transparencia incompatible con la competencia necesaria entre las entidades¹³³.

En resumen, la adopción de la inteligencia artificial plantea un gran desafío para los legisladores en el campo del Derecho de la competencia. El uso compartido de algoritmos entre competidores facilita la coordinación de precios sin necesidad de un acuerdo directo entre ellos, lo que crea un entorno propicio para prácticas anticompetitivas¹³⁴.

2.2. TRANSPARENCIA EN LA PUBLICIDAD ALGORÍTMICA

El denominado Reglamento de Mercados Digitales¹³⁵ trata de combatir la falta de transparencia en el contexto de las subastas de publicidad en tiempo real, pero no desde el punto de vista de los destinatarios, sino de los anunciantes y los editores¹³⁶.

La recopilación masiva de datos por parte de los gigantes tecnológicos como Google puede crear obstáculos a la libre competencia y dificultar la entrada de nuevos actores en el mercado. En efecto, al tener acceso a una gran cantidad de datos de las resultas de las consultas de los usuarios, este tipo de empresas pueden influir significativamente en el mercado, estableciendo barreras de acceso para los competidores.

Conforme preceptúa el art. 6 del citado Reglamento:

¹³² De 6 de noviembre de 2019. Disponible en https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.html?nn=48888.

¹³³ Resolución de 25 de noviembre de 2021. Se puede consultar en https://www.cnmc.es/sites/default/files/3831141_0.pdf.

¹³⁴ Tuset Varela, D., “El Impacto de la IA en el derecho de la competencia: breve análisis del caso Cornish-Adebisi, c. Caesars Entertainment”, *Diario La Ley Ciberderecho*, n° 84, junio 2024, consultado en versión digital en LEGALTECA.

¹³⁵ Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

¹³⁶ Sobre el deber de transparencia, vid. art. 5 núms. 9 y 10 DMA. Los “gatekeepers” deben proporcionar información, a diario y de forma gratuita, tanto a cada anunciante como a cada editor para quienes prestan servicios de publicidad en línea, sobre cada anuncio colocado. Ello incluye información separada sobre las tarifas pagadas por el anunciante y la remuneración correspondiente recibida por el editor, así como las métricas empleadas.

“2. El guardián de acceso no utilizará, en competencia con los usuarios profesionales, ningún dato que no sea públicamente accesible generado o proporcionado por dichos usuarios profesionales en el contexto de su uso de los servicios básicos de plataforma pertinentes o de los servicios prestados junto con los servicios básicos de plataforma pertinentes, o en apoyo de tales servicios, incluidos los datos generados o proporcionados por los clientes de dichos usuarios profesionales.

A los efectos del párrafo primero, los datos que no sean públicamente accesibles incluirán todos los datos agregados y desagregados generados por los usuarios profesionales que puedan inferirse o recopilarse a través de las actividades comerciales de los usuarios profesionales o sus usuarios finales, entre ellos los datos sobre los clics, las búsquedas, las visualizaciones y la voz, en los servicios básicos de plataforma pertinentes o en los servicios prestados junto con los servicios básicos de plataforma del guardián de acceso pertinentes, o en apoyo de tales servicios”.

La importancia práctica de estas restricciones, así como su conexión con el Derecho de la competencia se puede apreciar en la decisión del Tribunal de Justicia de la Unión Europea en el caso “Meta Platforms”¹³⁷ que tuvo su origen en un asunto planteado ante la Oficina Federal de la Competencia en Alemania. En este caso, el TJUE dictaminó que las autoridades nacionales de la competencia están legitimadas para investigar y sancionar infracciones del RGPD si dichas infracciones constituyen, a su vez, una explotación de posición dominante en el mercado. Además, se establecieron restricciones en relación con el tratamiento de datos dentro del grupo Meta con respecto a su servicio de publicidad personalizada. Estas restricciones afectan tanto al tratamiento de datos procedentes de varios servicios dentro del grupo Meta, como Facebook, Instagram o WhatsApp, como a los datos denominados “off-Facebook”. Estos últimos son datos recopilados por sitios web de terceros, aplicaciones o “social plugings”. De acuerdo con el Tribunal, ni la ejecución de un contrato ni el interés legítimo constituyen en este caso una base legal que legitime el tratamiento de datos de los usuarios en estos casos. Se necesitaría un consentimiento explícito e informado de los usuarios. Esto implica un cambio de modelo en relación con la publicidad en línea y los algoritmos de recomendación.

Otras acciones a destacar en relación con esta cuestión es la incoación de un procedimiento por parte de la Comisión el 25 de marzo de 2024 para investigar si el modelo de “pagar o consentir” introducido para los usuarios en la UE en noviembre de 2023 se ajusta a lo dispuesto en el art. 5 aparta-

¹³⁷ Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023 (ECLI:EU:C:2023:537).

do 2 del Reglamento de Mercados Digitales, precepto que impone sobre los guardianes de acceso, como Meta, la obligación de obtener el consentimiento de los usuarios cuando tengan previsto combinar los datos personales de los usuarios entre los servicios básicos de la plataforma y otros servicios. El 1 de julio de 2024 la Comisión envió sus conclusiones preliminares a Meta, informando de que su modelo publicitario de “pagar o consentir” incumple el Reglamento de Mercados Digitales. Se le ha concedido un plazo a Meta hasta el 1 de septiembre de 2024 para responder a las demandas de la Comisión y proponer soluciones. Si Meta no adopta las medidas necesarias, la Red de Cooperación para la Protección de los Consumidores puede adoptar medidas coercitivas, incluyendo sanciones.

Por otro lado, el diseño está llamado a desempeñar un gran papel a fin de que los usuarios finales puedan modificar la configuración del sistema operativo para evitar que sean dirigidos a productos o servicios del guardián de acceso. Así, conforme se establece en el art. 6.3 DMA:

“El guardián de acceso permitirá y posibilitará técnicamente a los usuarios finales desinstalar con facilidad cualquier aplicación informática del sistema operativo de dicho guardián de acceso, sin perjuicio de la posibilidad de que dicho guardián de acceso restrinja la desinstalación de aplicaciones informáticas preinstaladas que sean esenciales para el funcionamiento del sistema operativo o el dispositivo y que, desde un punto de vista técnico, no puedan ser ofrecidos de manera autónoma por terceros.

El guardián de acceso permitirá y posibilitará técnicamente a los usuarios finales modificar con facilidad la configuración por defecto del sistema operativo, del asistente virtual y del navegador web del guardián de acceso cuando estos dirijan u orienten a los usuarios finales hacia productos o servicios que ofrezca el guardián de acceso. Eso incluye solicitar a los usuarios finales, en el momento en que estos utilicen por primera vez un motor de búsqueda en línea, un asistente virtual o un navegador web del guardián de acceso que se enumere en la decisión de designación con arreglo al artículo 3, apartado 9, que elijan, de entre una lista de los principales prestadores de servicios disponibles, el motor de búsqueda en línea, el asistente virtual o el navegador al que el sistema operativo del guardián de acceso dirija u oriente a los usuarios por defecto, y el motor de búsqueda en línea al que el asistente virtual y el navegador del guardián de acceso dirijan u orienten a los usuarios por defecto”.

Asimismo, conforme al art. 6.5: “El guardián de acceso no tratará más favorablemente, ni en la clasificación ni en las funciones relacionadas de indexado y rastreo, a los servicios y productos ofrecidos por el propio guardián de acceso que a los servicios o productos similares de terceros. El guardián de

acceso aplicará condiciones transparentes, equitativas y no discriminatorias a dicha clasificación”.

Ello se aplica independientemente de los medios técnicos utilizados, lo que hace que el alcance sea muy amplio. En este sentido, el considerando (52) estipula que “(p)ara garantizar que esta obligación sea efectiva, las condiciones que se aplican a dicha clasificación también deben ser, en general, justas y transparentes. En este sentido, la clasificación debe comprender todas las formas de prominencia relativa, entre las que se incluyen la visualización, la valoración, la generación de enlaces o los resultados de voz...”.

Teniendo en cuenta que estos servicios tienen principalmente como finalidad la de mediar contenido (de terceros), la clasificación de este contenido suele ser el objeto principal del servicio (p.e. en las plataformas de vídeos o en los motores de búsqueda). Precisamente, la calidad de dicho servicio y su ventaja en el mercado se mide por lo bien que funciona la clasificación, la relevancia del contenido mostrado y la funcionalidad de los algoritmos subyacentes. Significa, sin duda, un paso adelante en términos de equidad y no discriminación, reemplazar el diseño de los algoritmos de clasificación (hasta ahora impulsado por intereses comerciales) dotándoles de componentes de interés social. Aunque es cierto que el art. 6.5 del Reglamento de Mercados Digitales no contiene especificaciones sobre lo que significa la transparencia en este sentido, sino más bien que las directrices a adoptar deberían facilitar la implementación y el cumplimiento de esta obligación (en las relaciones P2B), conforme se establece en el citado Considerando 52. En consecuencia, el Reglamento de Mercados Digitales aboga por un mayor grado de transparencia algorítmica.

3. DERECHO DE CONSUMO E INTELIGENCIA ARTIFICIAL

3.1. MICROTARGETING

Con la personalización masiva de anuncios dirigidos a los consumidores mediante inteligencia artificial (también conocida como “microtargeting”) estamos pasando de simples “trucos” en el diseño de la interfaz a estrategias verdaderamente sofisticadas¹³⁸.

¹³⁸ Franklin, M., Ashton, H., Gorman, R., Armstrong, S., “Missing Mechanisms of Manipulation in the EU AI Act”, *The International FLAIRS Conference Proceedings*, 2022, p. 2. En opinión de los autores, los sistemas de recomendación a menudo utilizan el aprendizaje automático (“machine lear-

El “microtargeting” se refiere al uso de la tecnología para perfilar específicamente a las personas en diferentes situaciones. Por ejemplo, se podría ajustar el precio de un producto o servicio según la presunta disposición del usuario a pagarlo¹³⁹. Esto podría basarse en factores como el modelo de su teléfono móvil, el nivel de batería del dispositivo o el número de visitas a una página web. Esta fijación dinámica de precios impulsada por la inteligencia artificial puede plantear problemas éticos, así como afectar a la crucial interacción entre el legítimo derecho a obtener beneficios económicos por parte de los agentes que operan en el mercado y el respeto a la transparencia y la equidad esenciales para la protección de los consumidores¹⁴⁰. Como se ha señalado anteriormente, la normativa de protección de los consumidores¹⁴¹ inspirada en un contexto socioeconómico y técnico específico, no siempre se adapta de la mejor manera a los desafíos que plantea la inteligencia artificial¹⁴².

El Consejo de Europa publicó ya en 2019 una declaración sobre las capacidades de manipulación de los procesos algorítmicos¹⁴³. También la Comisión europea advirtió sobre el creciente poder de los algoritmos para influir subliminalmente en las decisiones humanas y en cuestiones importantes que inter-

ning”, ML) para aprender las preferencias de los usuarios y optimizar la entrega de algún servicio. Cuando se aplica un enfoque de aprendizaje automático interactivo a los sistemas de recomendación se vuelve cada vez más difícil identificar si el sistema está aprendiendo realmente las preferencias de los usuarios o si el sistema de recomendación está influenciando a los usuarios para que comporten de cierta manera con el fin de maximizar su función. En la misma línea cfr. Azzutti, A., “AI trading and the limits of EU law enforcement in deterring market manipulation”, *Computer Law & Security Review*, 45, 2022, p. 5; Boine, C. “AI-enabled manipulation and EU law”, 2021, p. 5.

¹³⁹ Vid. Diario ABC 2 septiembre 2024: “¿Cuál es tu precio?” (Todos tenemos uno. Y las empresas lo saben”. Conforme se recoge en el texto de la noticia: “Quizá no lo sepas, pero si compras *on-line* unos zapatos antes de las siete de la tarde, pagarás más por ellos, y si vives en un barrio de clase alta, nunca recibirás una oferta de auriculares baratos. Los precios estandarizados y las rebajas de toda la vida han dado paso en Internet a estrategias mucho más complicadas, diseñadas para “exprimir” al consumidor”.

¹⁴⁰ Gazi, M. S., Hasan, M. R., Gurung, N., & Mitra, A., “Ethical Considerations in AI-driven Dynamic Pricing in the USA: Balancing Profit Maximization with Consumer Fairness and Transparency”, *Journal of Economics, Finance and Accounting Studies*, 6(2), 2024, pp. 100-111. Jablonowska, A., Kuziemski, M., Nowak, A. M., Micklitz, H. W., Palka, P., & Sartor, G., “Consumer law and artificial intelligence”, *EUI Department of Law Research Paper*, 11, 2018, <https://artsy.eui.eu/wp-content/uploads/sites/37/2018/07/ARTSY-Final-Report.pdf>.

¹⁴¹ En concreto, para el Derecho español según propone Argelich Comelles, C., “Contratación con inteligencia artificial y contratos algorítmicos: repensando el Derecho civil ante el informe español de la legislación de consumo y mercantil para la Comisión Europea”, *Rev. Crítica de Derecho Inmobiliario*, N.º 804, 2024, p. 2044: “En relación con los *dynamic pricing algorithms*, o aquellos algoritmos que para modificar los precios utilizan la IA, y la manipulación de precios (...), deben modificarse el art. 60.1 c), y el art. 97.1 e) y f) TRLGDCU en el sentido de impedir que, si el precio no puede calcularse razonablemente con antelación, sea posible determinarlo después de la celebración del contrato”.

¹⁴² Księżak, P., & Wojtczak, S., *Toward a conceptual network for the private law of artificial intelligence* (Vol. 51). Springer, 2023, p. 5.

¹⁴³ Adoptada por el Consejo de Ministros el 13 de febrero de 2019. Se puede consultar en <https://search.coe.int/cm?i=090000168092dd4b>.

fieren con el principio de autonomía personal¹⁴⁴. La denominada responsabilidad algorítmica (“algorithmic accountability”) presenta, sin duda, enormes retos para el legislador.

Los profesionales que operan en el mercado digital a menudo diseñan técnicas para influir en el comportamiento de los usuarios de una manera no evidente. Estas técnicas incluyen el empleo de algoritmos sofisticados o inteligencia artificial, aprovechando experiencias personalizadas. El desafío radica en descubrir y comprender cómo operan estos sistemas bajo la superficie para influir en las decisiones de los usuarios, lo que requiere un alto grado de especialización técnica¹⁴⁵.

En el actual art. 5.1 Reglamento de Inteligencia Artificial¹⁴⁶ se establece que estarán prohibidas las siguientes prácticas de inteligencia artificial:

“a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un grupo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que una persona tome una decisión que de otro modo no habría tomado, de un modo que provoque, o sea probable que provoque, perjuicios considerables a esa persona, a otra persona o a un grupo de personas”¹⁴⁷.

La manipulación digital del consumidor puede erosionar la autonomía privada, limitar la competencia, al margen de violar la privacidad y comprometer la dignidad personal de los consumidores¹⁴⁸.

¹⁴⁴ Vid. Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence, 21.04.2021. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084>.

¹⁴⁵ Azzutti, A., “AI trading and the limits of EU law enforcement in deterring market manipulation”, *Computer Law & Security Review*, 45, 2022, p. 2. En opinión del autor, la reacción frente a estos abusos se vuelve ineficaz si no puede identificarse a las personas responsables, ya que puede ser difícil establecer su grado de responsabilidad en la causación del daño por su mala conducta debido a la implementación manipuladora de estrategias de comercio algorítmico.

¹⁴⁶ Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

¹⁴⁷ El Parlamento presentó la enmienda 84 a la Propuesta de Reglamento sobre Inteligencia artificial en el sentido de introducir un nuevo Considerando 47 bis: “Dichos requisitos en materia de transparencia y de explicabilidad de la toma de decisiones por la IA también deben ayudar a contrarrestar los efectos disuasorios de la asimetría digital y los llamados «patrones oscuros», dirigidos contra las personas y su consentimiento informado”.

¹⁴⁸ Vid. Manwaring, K., “Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation”, *Competition and Consumer Law Journal*, 2018, pp. 141-181.

3.2. CONTRATOS ALGORÍTMICOS

Vivimos en un momento en el que los asistentes digitales y las plataformas tecnológicas recopilan una ingente cantidad de datos sobre nosotros. Estos datos, obtenidos muchas veces de manera inconsciente, pueden tener un gran impacto en nuestra experiencia en línea y en la toma de decisiones. Pensemos en el asistente digital que observa las preferencias del usuario, las búsquedas, los clics... y va creando un perfil con el fin de personalizar anuncios, recomendaciones de contenido, noticias, etc. El problema se presenta cuando las corporaciones utilizan estos datos para dirigir a los usuarios hacia ciertos productos en función de sus intereses comerciales y con técnicas manipuladoras¹⁴⁹.

Resulta de mucho interés en este ámbito el Informe Provisional de “European Law Institute” sobre Principios Rectores y Modelos de Reglas sobre Contratos Algorítmicos que se centra en el uso de la toma de decisiones automatizada (ADM) a través de algoritmos, especialmente aquellos impulsados por inteligencia artificial (IA), para la conclusión y/o ejecución de contratos.

Este informe provisional proporciona ocho principios generales que deben guiar la adaptación del Derecho Europeo de Consumo existente a la toma de decisiones automatizada (ADM). Además, en la última parte del informe se analizan las Directivas clave de Derecho de consumo de la UE¹⁵⁰ para explicar dónde puede haber necesidad de enmendar o complementar la correspondiente Directiva para garantizar que dé cobertura a la implementación de asistentes digitales por parte de los consumidores en algunos de los pasos hacia la conclusión y ejecución de un contrato. También se explora cómo se deben aplicar las disposiciones actuales a situaciones en las que se emplean asistentes digitales.

Volviendo a los principios, en el segundo de ellos se establece que se aplica el Derecho de consumo a los contratos algorítmicos. Una consecuencia lógica de este enfoque es que el contrato concluido a través de un asistente digital será entre un consumidor y un comerciante, y, por lo tanto, estará sujeto al Derecho de consumo de la UE. De este modo, los asistentes digitales deberían diseñarse en función del marco legal vigente (por ejemplo, en lo que respecta a los deberes de información)¹⁵¹.

¹⁴⁹ Stucke, M. E., & Ezrachi, A., “How digital assistants can harm our economy, privacy, and democracy”, *Berkeley Technology Law Journal*, 32(3), 2017, pp. 1239-1300.

¹⁵⁰ En concreto, el informe se refiere a: Unfair Contract Terms Directive (93/13/EEC); E-Commerce Directive (2000/31/EC); Unfair Commercial Practices Directive (2005/29/EC); Consumer Rights Directive (2011/83/EU); Proposal for Amending the Consumer Rights Directive Regarding Financial Services Contracts Concluded at a Distance; Directives on Consumer Sales (2019/771/EU) and Digital Content/Digital Services (2019/770/EU)

¹⁵¹ Twigg-Flesner, C., Rodríguez de las Heras Ballell, T., Busch, C., Jull Sørensen, M., & Szostek, D., EU Consumer Law and Automated Decision-Making: Is EU Consumer Law ready for ADM, 2023, p. 10.

Merece destacarse, teniendo en cuenta el tema que nos ocupa, el principio 6 referido a la protección frente a la manipulación. En opinión de los autores, el actual Derecho de consumo de la UE ya pretende prevenir la manipulación de los consumidores al decidir si deben concluir un contrato y en qué términos, así como al ejercer sus derechos contractuales. Esta protección debería extenderse para abarcar los intentos de manipulación de un asistente digital¹⁵².

Según los autores de los principios, la protección del consumidor podría requerir de un mayor desarrollo en el ámbito de la contratación algorítmica. Cuando las decisiones de consumo ya no son tomadas directamente por los consumidores, sino por asistentes digitales (empleados por los consumidores y teniendo en cuenta sus datos personales), estos sistemas deben estar protegidos contra la manipulación dirigida, por ejemplo, a través de los llamados “ataques adversarios” (“adversarial attacks”)¹⁵³ que pueden causar una clasificación errónea por parte de un asistente digital. Otro riesgo de manipulación surge de las llamadas “inyecciones de indicaciones” (“prompt injections”), que podrían manipular la forma en que un sistema de IA procesa los datos que utiliza para tomar decisiones. Las reglas de diseño para los sistemas de IA en general o los asistentes digitales en particular podrían estipular que se incorporen medidas tecnológicas para minimizar tales riesgos¹⁵⁴.

4. BIBLIOGRAFÍA

ARGELICH COMELLES, C. (2024). “Contratación con inteligencia artificial y contratos algorítmicos: repensando el Derecho civil ante el informe español de la legislación de consumo y mercantil para la Comisión Europea”, *Rev. Crítica de Derecho Inmobiliario*, N.º 804, pp. 2033-2071.

AZZUTTI, A. (2022). “AI trading and the limits of EU law enforcement in deterring market manipulation”. *Computer Law & Security Review*, 45, <https://doi.org/10.1016/j.clsr.2022.105690>.

BOINE, C. (2021). “AI-enabled manipulation and EU law”. disponible en <https://ssrn.com/abstract=4042321> o <http://dx.doi.org/10.2139/ssrn.4042321>

¹⁵² Twigg-Flesner, C., Rodríguez de las Heras Ballell, T., Busch, C., Jull Sørensen, M., & Szostek, D., EU Consumer Law and Automated Decision-Making: Is EU Consumer Law ready for ADM, 2023, p. 11.

¹⁵³ Los ataques adversarios en la inteligencia artificial son una técnica que explota las vulnerabilidades de los modelos de aprendizaje automático para manipular su comportamiento.

¹⁵⁴ Twigg-Flesner, C., Rodríguez de las Heras Ballell, T., Busch, C., Jull Sørensen, M., & Szostek, D., EU Consumer Law and Automated Decision-Making: Is EU Consumer Law ready for ADM, 2023, p. 31.

- COLE, M. D.; ETTELDORF, C., SCHMITZ, S., UKROW, J. (2023). "Algorithmic transparency and accountability of digital services", European Audiovisual Observatory, Strasbourg.
- DEMELIS, N. (2024). "The Antitrust Alphabet: Amazon, Buy Box, and Competition", *Boston College Intellectual Property and Technology Forum*, pp. 1-27.
- FRANKLIN, M., ASHTON, H., GORMAN, R., & ARMSTRONG, S. (2022, May). "Missing mechanisms of manipulation in the EU AI Act". In *The International FLAIRS Conference Proceedings* (Vol. 35).
- GAZI, M. S., HASAN, M. R., GURUNG, N., & MITRA, A. (2024). "Ethical Considerations in AI-driven Dynamic Pricing in the USA: Balancing Profit Maximization with Consumer Fairness and Transparency", *Journal of Economics, Finance and Accounting Studies*, 6(2), pp. 100-111.
- GROCHOWSKI, M., JABLONOWSKA, A., LAGIOIA, F., SARTOR, G. (2021). "Algorithmic transparency and explainability for eu consumer protection: unwrapping the regulatory premises". *Critical Analysis of Law: An International & Interdisciplinary Law Review*, 8(1), pp. 43-63.
- JABLONOWSKA, A., KUZIEWSKI, M., NOWAK, A. M., MICKLITZ, H. W., PAŁKA, P., & SARTOR, G. (2018). "Consumer law and artificial intelligence". *EUI Department of Law Research Paper*, 11.
- KSIEŻAK, P., & WOJTCZAK, S. (2023). *Toward a conceptual network for the private law of artificial intelligence* (Vol. 51), Springer.
- MANWARING, K. (2018). "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation", *Competition and Consumer Law Journal*, pp. 141-181.
- MARTY, F. (2024). *Les collusions algorithmiques: mythe ou réalité?* disponible en: www.ofce.sciences-po.fr/pdf/dtravail/WP2024-09.pdf.
- STUCKE, M. E., & EZRACHI, A. (2017). "How digital assistants can harm our economy, privacy, and democracy", *Berkeley Technology Law Journal*, 32(3), pp. 1239-1300.
- TUSET VARELA, D. (2024). "El Impacto de la IA en el derecho de la competencia: breve análisis del caso Cornish-Adebiyi, c. Caesars Entertainment", *Diario La Ley Ciberderecho*, n.º 84, consultado en versión digital en LEGALTECA.
- TWIGG-FLESNER, C., RODRÍGUEZ DE LAS HERAS BALLELL, T., BUSCH, C., JULL SØRENSEN, M., & SZOSTEK, D. (2023). "EU Consumer Law and Automated Decision-Making: Is EU Consumer Law ready for ADM?", Disponible en: *SSRN 4667682*.
- VINOD, B. (2024). "What is the future of competitive revenue management in the travel industry?", *Journal of Revenue and Pricing Management*, pp. 1-3.
- ZINGALES, N. (2018). "Google Shopping: beware of 'self-favouring' in a world of algorithmic nudging", *Competition Policy International-Europe Column*. Disponible en <https://ssrn.com/abstract=3707797>.

Uso de inteligencia artificial, *Big Data* y otras tecnologías disruptivas en las plataformas digitales de alojamiento turístico: desafíos actuales en materia de privacidad, transparencia algorítmica y responsabilidad civil¹

LUCÍA MOLINA MARTÍNEZ

*Profesora Ayudante Doctora de Derecho Civil
Universidad de Alicante*

Sumario: 1. *BIG DATA*, INTELIGENCIA ARTIFICIAL, IOT Y TECNOLOGÍA *BLOCKCHAIN* EN LAS PLATAFORMAS DIGITALES DE ALOJAMIENTO TURÍSTICO. 1.1. La transformación digital del sector turístico: el papel de las plataformas digitales de alojamiento turístico. 1.2. La aplicación de tecnologías innovadoras disruptivas por las plataformas de alojamiento turístico: desde el algoritmo hasta la tecnología *blockchain*. 2. IMPACTO DE LAS TECNOLOGÍAS DISRUPTIVAS EN LA PRIVACIDAD Y PROTECCIÓN DE DATOS EN LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO. 2.1. Empleo de tecnologías disruptivas en la recopilación y tratamiento masivo de datos personales: aparición de nuevas categorías de datos y riesgos para la privacidad de los usuarios. 2.2. La elaboración de perfiles y la adopción de decisiones automatizadas a través de sistemas avanzados de IA. 3. TRANSPARENCIA ALGORÍTMICA Y RESPONSABILIDAD CIVIL EN EL MARCO DE LA INTERMEDIACIÓN DE LAS PLATAFORMAS DE

¹ Trabajo realizado al amparo de los Proyectos «La irrupción de la inteligencia artificial en el Derecho de daños y su adaptación a las nuevas tecnologías» - Referencia PID2020-116185GB-I00 (Ministerio de Ciencia e Innovación - Agencia Estatal de investigación) y «La Unión Europea ante los desafíos regulatorios de la Inteligencia Artificial: cuestiones de responsabilidad civil» - CIGE/2023/196 (Conselleria d'Educació, Cultura, Universitats i Ocupació de la Generalitat Valenciana).

ALOJAMIENTO TURÍSTICO 3.1. Desafíos que plantea la toma de decisiones algorítmicas y la regulación europea en materia de IA para combatirlos. 3.2. Exigencias de transparencia para los sistemas algorítmicos de recomendación, clasificación, selección de contenidos y publicidad en línea de los prestadores de servicios de alojamiento de datos. 3.3. Tratamiento legal de la responsabilidad de las plataformas por la moderación automatizada de contenidos y el incumplimiento de las obligaciones de transparencia algorítmica: régimen transitorio a la espera de una regulación específica acerca de la discriminación algorítmica. BIBLIOGRAFÍA

1. *BIG DATA*, INTELIGENCIA ARTIFICIAL, IoT Y TECNOLOGÍA *BLOCKCHAIN* EN LAS PLATAFORMAS DIGITALES DE ALOJAMIENTO TURÍSTICO

1.1. LA TRANSFORMACIÓN DIGITAL DEL SECTOR TURÍSTICO: EL PAPEL DE LAS PLATAFORMAS DIGITALES DE ALOJAMIENTO TURÍSTICO

En los últimos años, hemos asistido a un espectacular desarrollo tecnológico protagonizado por el avance de la Inteligencia Artificial (IA). Su evolución, desde los sistemas clásicos o simbólicos, que utilizaban reglas lógicas y estructuras predefinidas, hasta las técnicas más modernas que emplean grandes volúmenes de datos -*Big Data*- y se basan en el aprendizaje automático, ha supuesto un cambio de paradigma para la industria, al proporcionar poderosas herramientas para la optimización, la personalización y la innovación. La implementación de esta y otras herramientas disruptivas, tales como el *Internet of Things* (IoT) o la tecnología *blockchain*, ha provocado una acelerada transformación digital de la industria, que implica la redefinición de los propios modelos de negocio, y que marca el inicio de lo que se conoce como «Cuarta Revolución Industrial»².

El sector turístico, cuya evolución indefectiblemente va unida a la consolidación de la economía digital³, es uno de los sectores que mayor transformación está experimentando como consecuencia de esta revolución tecnológica⁴. Así, desde la aparición del *e-commerce* hasta nuestros días, la industria

² Así se ha bautizado a este fenómeno, una revolución tecnológica sin precedentes que promete cambiar todo aquello que nos rodea. Al respecto, Schwab (2016: 19-28).

³ Hojehghan y Esfangareh (2011: 308-316).

⁴ Según el último informe de la Organización para la Cooperación y el Desarrollo Económico (2024: 40), el papel transformador que la IA y otras tecnologías innovadoras puede tener en el sector del turismo es fundamental para el crecimiento económico; sin embargo, este aún no ha sido explo-

turística ha vivido un proceso de adaptación continua, promovido por las tecnologías digitales disruptivas, que ha dado lugar a la remodelación del sector y, con ello, a la aparición de un turismo inteligente soportado íntegramente en los datos y su tratamiento. Las últimas tendencias hablan, de hecho, de una nueva etapa en la industria del turismo, el *e-Tourism*⁵, donde las tecnologías disruptivas pasan a ocupar un papel central en las distintas actividades que engloba el sector turístico, desde la búsqueda de información y reservas *online* hasta la gestión de destinos y la personalización de experiencias. Gracias a tecnologías complejas y avanzadas, como la IA, el *Big Data*, la realidad virtual y aumentada, los *chatbots*, la tecnología *blockchain*, los drones, el IoT o el metaverso, el sector turístico es ahora capaz de ofrecer experiencias más personalizadas, eficientes e inmersivas, optimizando los recursos y transformando la forma en la que el cliente turístico planifica, reserva y disfruta de sus viajes⁶.

En esta etapa de digitalización y automatización del sector turístico desempeñan un papel crucial las plataformas digitales⁷, en la medida en que, desde hace ya algunos años, se han consolidado como el epicentro de la oferta y la demanda de servicios. La rápida expansión de estas plataformas ha venido, sin duda, propulsada por varios factores tecnológicos clave, tales como la llegada de los *smartphones* y sus sistemas de geolocalización, la aparición de sistemas de pago *online* seguro o la utilización de la analítica *Big Data*; factores, todos ellos, que han hecho más visibles y accesibles estas plataformas para los usuarios al tiempo que han aumentado la efectividad y competitividad de las mismas⁸.

rado del todo. Precisamente por ello, el Grupo de Turismo del G7 ha asumido la función de investigar las implicaciones de la IA en este sector y la formulación de políticas turísticas. Al mismo tiempo, muchos países han comenzado a apoyar la investigación y el desarrollo de la IA en el sector turístico. En esta dirección, España, en 2022, invirtió 45 millones de euros para impulsar la adopción de la IA en las empresas turísticas y destinó 115 millones a la promoción del desarrollo digital de los destinos turísticos. Como fruto de esta inversión, se ha creado un Programa de Digitalización e Inteligencia para que los destinos y las empresas turísticas desarrollen plataformas de destinos inteligentes, y ello con el objetivo de ofrecer a los turistas servicios públicos y privados interoperables.

⁵ Véase, al respecto, Gretzel *et al.* (2015: 180-182). Para Más Ferrando, Ramón Rodríguez y Aranda Cuéllar (2020: 230-232), este cambio de paradigma tecnológico representa una oportunidad para el turismo en España, quien debe apostar de manera decidida por la innovación para aumentar su competitividad y mantener una posición de liderazgo en el largo plazo.

⁶ Sobre las aplicaciones actuales y potenciales de estas tecnologías en el sector turístico, pueden verse los estudios de Ramón Fernández (2022: 37-68) y Pacheco Jiménez (2023: 26-35).

⁷ Para una aproximación al fenómeno de las plataformas digitales, se recomienda el estudio de Rodríguez de las Heras Ballell (2019: 93-127).

⁸ El altísimo potencial de las plataformas para la creación de valor digital fue puesto de manifiesto por la Comisión Europea en su Comunicación de 25 de mayo de 2016, quien, sin perjuicio de reconocer la existencia de diferentes tipologías de plataformas y sus rápidas transformaciones, extrajo una serie de características que todas ellas comparten: en primer lugar, las plataformas son capaces de crear y modelar nuevos mercados, además de facilitar nuevas formas de participación o llevar a

Dentro del fenómeno de las plataformas turísticas, han tenido una muy relevante proyección las del sector del alojamiento turístico, como son Booking, Airbnb, Tripadvisor, Vrbo, Windu o Expedia, por citar las más conocidas⁹. La tradicional forma de reservar y contratar un alojamiento, contactando de forma directa con el propietario del alojamiento o a través de agencias de viaje, ha sido reemplazada por el empleo de estas plataformas, las cuales actúan como intermediarias en línea para la contratación de alojamientos turísticos o hoteleros, facilitando la conexión entre los oferentes y los demandantes de tales servicios¹⁰. El éxito de estas plataformas radica en que funcionan como mercados electrónicos (*marketplaces*) en línea altamente eficientes y competitivos gracias al uso de la tecnología digital, la conectividad global y los datos. Entre sus funcionalidades se incluyen las herramientas de búsqueda y comparación que permiten a los usuarios filtrar opciones según sus preferencias

cabo negocios centrados en la recogida, tratamiento y análisis de grandes volúmenes de datos; en segundo lugar, operan en mercados multifacéticos, aunque pueden ejercer diferentes grados de control sobre la relación subyacente entre los usuarios; en tercer lugar, se benefician de los «efectos de red», lo que implica que el valor del servicio aumenta a medida que crece el número de usuarios; en cuarto lugar; se apoyan en tecnologías de la información y la comunicación para llegar a sus usuarios de forma instantánea y sin esfuerzo; y, por último, desempeñan un papel fundamental en la generación de valor digital, especialmente a través de la acumulación de datos, impulsando nuevos proyectos empresariales y generando nuevas dependencias estratégicas (apdo. 2). Véase, la Comunicación al Parlamento Europeo, el Comité Económico y Social Europeo y al Comité de las Regiones de 25 de mayo de 2016 [COM (2016) 288 final].

⁹ Entre estas plataformas, encontramos algunas que intermedian en el arrendamiento de viviendas y apartamentos turísticos, como Airbnb o Vrbo, cuyo principal mercado es la mal llamada «economía colaborativa», y otras, como Booking o Expedia, que son plataformas de reservas de alojamientos hoteleros en las que el oferente siempre será un profesional. Hace ya tiempo que la doctrina ha advertido que aquellas plataformas que surgieron con carácter colaborativo se están llenando de profesionales en el lado de la oferta y que no son sostenibles para los particulares cuando existen costes de transacción significativos. Véase, al respecto, Alfaro Águila-Real (2 de mayo de 2016). En el presente estudio, y atendiendo a la desnaturalización de la «economía colaborativa» a la que asistimos, preferimos abordar el fenómeno de la «economía de plataformas», tomando como denominador común la utilización de una plataforma virtual donde se encuentran la oferta y la demanda de servicios de alojamiento turístico o hotelero, sin perjuicio de que en esas plataformas puedan darse relaciones contractuales entre particulares o entre profesional y consumidor. Ahora bien, un aspecto que debe quedar claro desde un primer momento es que el modelo de plataformas B2C y el modelo C2C (o P2P) es necesariamente distinto y algunos textos normativos promulgados en este sector de la economía solo son de aplicación en los modelos B2C, es decir, cuando quien oferta el alojamiento es empresario. Así ocurre, como se verá, con el Reglamento (UE) 2019/1150, de 20 de junio, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (RE-P2B). Sobre esta distinción, entre los trabajos más recientes, Martínez Nadal (2022b: 57-84) y Mate Satué (2023: 113-114).

¹⁰ Estas plataformas aglutinan en la actualidad prácticamente la totalidad de las ofertas del sector y se espera que su auge vaya en aumento. Según los últimos datos de Eurostat, durante el primer trimestre de 2024, se produjeron 123,7 millones de reservas a través de plataformas digitales, lo que supone un incremento del 28,3 % con respecto al mismo período del año anterior. Puede consultarse en: <https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20240729-1> [último acceso: 3-9-2024].

y necesidades, pagos electrónicos seguros que facilitan las transacciones rápidas, mecanismos de resolución de conflictos y sistemas de reputación que ofrecen reseñas y comentarios para asegurar la calidad y la confianza en el alojamiento¹¹. Estas plataformas tienen, además, la capacidad de conectar de manera masiva -en ocasiones, incluso en tiempo real- la oferta y la demanda, lo que hacen a través del análisis de una enorme cantidad de datos obtenidos del perfil de los usuarios, sus preferencias, los registros del equipo desde el que accede y de los macrodatos. Toda esta información es procesada y combinada por complejos algoritmos matemáticos, permitiendo una intermediación eficiente entre el proveedor y el destinatario desde la puesta de ambos en contacto hasta la gestión del pago y la calificación cruzada.

1.2. LA APLICACIÓN DE TECNOLOGÍAS INNOVADORAS DISRUPTIVAS POR LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO: DESDE EL ALGORITMO HASTA LA TECNOLOGÍA *BLOCKCHAIN*

Los datos, en la medida en que maximizan la labor de intermediación de las plataformas, constituyen un importante activo económico para ellas¹², lo que explica que toda su actividad grave en torno a la recopilación y el tratamiento masivo de los datos que recaban. Desde este prisma, los datos vendrían a ser una suerte de materia prima (*raw data*), que, tras pasar por diversas técnicas de procesamiento masivo, genera conocimiento útil aplicable a múltiples actividades, desde la casación de la oferta y la demanda o la fijación de precios, hasta la elaboración de publicidad personalizada¹³.

En los últimos años, la producción de datos ha crecido de manera exponencial gracias al rastro de navegación que dejan los usuarios en internet

¹¹ Rodríguez Martínez (2017:195).

¹² Los datos se han consagrado como un elemento vital para el desarrollo económico y social, ya que son la base de nuevos productos y servicios, impulsan la productividad y la eficiencia de muchos sectores económicos, facilitan la toma de decisiones, permiten la creación de productos y servicios más personalizados, contribuyen a la modernización de servicios gubernamentales, etc. Precisamente por ello, la Comisión Europea puso en marcha en 2020 la Estrategia Europea de Datos, la cual reconoce el valor fundamental de los datos para el progreso y pone el foco en aprovechar su potencial para impulsar la innovación y la competitividad. El objetivo último de esta Estrategia es convertir a la Unión Europea en líder global de la economía basada en datos. Véase, la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Una Estrategia Europea en materia de datos», de 19 de febrero de 2020 [COM (2020) 66 final], pp. 1-5.

¹³ Como explica Castillo Parrilla (2020: 122-123), la utilización económica de los datos genera una cadena de valor muy parecida a la de cualquier otra materia prima, con la particularidad de que en este caso la materia prima sería la información desnuda, y los instrumentos para el procesamiento, los algoritmos.

(huella digital) cuando utilizan dispositivos tecnológicos. Las plataformas digitales de alojamiento turístico, conscientes de que ello representa una fuente potencial de crecimiento e innovación que debe aprovecharse, han desarrollado e implementado tecnologías del ámbito de la IA cada vez más innovadoras y disruptivas que posibilitan el tratamiento masivo de esos datos (*Big Data*)¹⁴. Dichas innovaciones, por un lado, han incrementado las fuentes de datos disponibles y, por otro, han simplificado el análisis de las correlaciones entre estos datos, la realización de predicciones y la toma de decisiones en tiempo real¹⁵.

Entre las soluciones tecnológicas más importantes que se han implementado en el sector turístico, y que mayores avances están experimentando, debe destacarse el empleo de técnicas de IA de aprendizaje automático o *machine learning* y de aprendizaje profundo o *deep learning*, el uso del IoT o la aplicación de tecnología *blockchain*.

El aprendizaje automático o *machine learning* hace referencia a una amplia gama de algoritmos que proporcionan a los sistemas de IA la capacidad de aprender de forma automática de conjuntos de datos preexistentes sin estar programados para ello, es decir, sin necesidad de basarse en reglas previamente codificadas¹⁶. Como ha subrayado la Agencia Española de Protección de Datos (2020: 6), a través de esta herramienta tecnológica se diseñan modelos predictivos que establecen por sí solos la relación entre las variables mediante el análisis del conjunto inicial de datos, la identificación de patrones y la creación de criterios de clasificación. Una vez definidos estos criterios, el componente IA realizará inferencias sobre los nuevos conjuntos de datos que sean introducidos. Dentro del aprendizaje automático, podemos encontrar diferentes técnicas, que varían en complejidad y autonomía, como son el aprendizaje supervisado, el aprendizaje no supervisado, el aprendizaje semi-supervisado, el aprendizaje por refuerzo o el aprendizaje federado¹⁷.

El aprendizaje profundo o *deep learning*, por su parte, es una especialización del aprendizaje automático, cuya principal base tecnológica son los algoritmos de redes neuronales que aspiran a imitar el comportamiento de las neuronas del cerebro humano. Estas redes tienen la capacidad de identificar patrones ocultos y establecer correlaciones inesperadas a través del análisis masivo de grandes volúmenes de datos, generando de forma automática

¹⁴ El término *Big Data* incluye, de hecho, estos dos elementos: por un lado, el gran volumen de datos disponibles y, por el otro, el empleo de tecnologías que se sirven de complejos algoritmos para tratar esa gran cantidad de información y extraer de ella correlaciones y predicciones que facilitan la toma de decisiones. Al respecto, Beltrán Pardo y Sevillano Jaén (2013: 16).

¹⁵ Gutiérrez David (2021: 69).

¹⁶ Barrios Andrés (2020: 59).

¹⁷ Para una descripción de cada una de estas técnicas, véase Domínguez Álvarez (2024: 54-57).

los modelos predictivos que posteriormente aplican a nuevos conjuntos de datos¹⁸. A diferencia de otras técnicas de aprendizaje automático, como el aprendizaje supervisado, que requieren realizar manualmente los procesos de extracción de características y el diseño de un modelo para categorizar la información objeto de análisis, el aprendizaje profundo lo hace de manera automática a partir de imágenes, textos o sonidos, lo que, a juicio de Barrios Andrés (2020: 62), lo convierte en una técnica especialmente precisa y que puede, incluso, superar al rendimiento humano. Sin embargo, como ha advertido Sánchez Caparrós (2022: 4), el aprendizaje profundo representa también un gran desafío para los derechos humanos, en la medida en que su propia naturaleza conlleva que no se pueda explicar la multitud de correlaciones que se procesan en las capas ocultas y, en lógica consonancia, que no podamos entender por qué un sistema se ha comportado de un determinado modo o ha ofrecido una respuesta específica.

En línea con lo expuesto, debe advertirse que muchas de las tareas que llevan a cabo las plataformas de alojamiento turístico, tales como la recomendación de un alojamiento, la fijación del precio, la clasificación de las ofertas o la filtración de comentarios, viene determinada por el tratamiento de datos personales que estas llevan a cabo mediante algoritmos de aprendizaje automático y, con menor frecuencia, de aprendizaje profundo. Estos algoritmos son capaces de predecir con precisión la probabilidad de que un oferente acepte una solicitud de reserva o que un usuario evalúe positivamente una experiencia, ya que analizan de manera eficiente las preferencias individuales, ofreciendo alojamientos que se adaptan de manera óptima a las expectativas de cada usuario, lo que contribuye significativamente a mejorar su experiencia y satisfacción. En sus políticas de privacidad, plataformas como Vrbo¹⁹ o Expedia²⁰ advierten sobre el empleo algoritmos de aprendizaje automático para llevar a cabo algunas de estas tareas:

«Usamos la inteligencia artificial y el aprendizaje automático con diversos fines para ofrecer nuestra plataforma y los servicios asociados. Podemos usar tus datos personales con los siguientes fines: Para mejorar tu experiencia como usuario y mantener nuestro sitio web seguro; Para determinar el orden de clasificación que ves en nuestro sitio web; Para proporcionar recomendaciones de destinos, alojamientos o actividades; Para filtrar el contenido que cargas en nuestro sitio web (por ejemplo, imágenes de tus alojamientos) y garantizar que cumple con nuestros requisitos de calidad o de

¹⁸ Así lo explica Solar Cayón (2020: 148).

¹⁹ Véase el apartado «Nuestro uso de la inteligencia artificial» de su política de privacidad. Disponible en: <https://www.vrbo.com/es-es/lp/b/privacy-policy> [último acceso: 3-9-2024].

²⁰ Véase el apartado «Nuestro uso de la inteligencia artificial» de su política de privacidad. Disponible en: <https://www.expedia.es/lp/b/privacy> [último acceso: 3-9-2024].

formato, y para identificar los servicios pertinentes que se incluyen en tu anuncio; Para filtrar los comentarios que compartes con nosotros y garantizar que no contienen datos personales identificables o para valorar la satisfacción del cliente ... [...]».

Por su parte, Airbnb, que siempre ha estado a la vanguardia de la innovación tecnológica, emplea procesamiento del lenguaje natural (NLP, por sus siglas en inglés) sobre los comentarios de los huéspedes, la interacción entre sus usuarios y la descripción de los anfitriones, y ello con la finalidad de obtener más información y optimizar su servicio²¹. Asimismo, una de sus innovaciones más exitosas ha sido la aplicación de algoritmos de aprendizaje profundo para la clasificación de las búsquedas²². Recientemente, hemos tenido noticia de que Booking, que también ha realizado una fuerte apuesta por la IA, ha desarrollado un planificador de viajes, que funciona parcialmente gracias a la tecnología de los modelos de lenguaje de la API Chat GPT de OpenAI, y que tiene como objetivo ayudar a las personas a planificar y organizar sus viajes creando una experiencia de conversación innovadora²³. Las herramientas de planificación de viajes asistidas por IA generativa, que requieren el empleo de avanzadas técnicas de aprendizaje profundo, son cada vez más comunes, y otras plataformas, como Expedia o Tripadvisor, también han apostado por ellas²⁴.

Otra de las aplicaciones más relevantes de los algoritmos de aprendizaje automático y profundo en el sector del alojamiento turístico consiste en el análisis de los hábitos, preferencias y sensibilidad de cada usuario para la elaboración de publicidad personalizada. Este es el caso, por ejemplo, de plataformas como Booking²⁵ y Wimdu²⁶, que se sirven a este fin de la tecnología Criteo, la cual, por medio de un algoritmo, analiza el comportamiento de navegación, lo que permite mostrar recomendaciones dirigidas en forma de anuncios personalizados en otros sitios web. Esta técnica de marketing, que permite orientar la elección final del consumidor en función de sus hábitos y

²¹ Pese a que nada indica en su política de privacidad, lo advirtieron, hace ya unos años, Laurent *et al.* (2015: 4).

²² Se han hecho eco de ello Halдар *et al.* (2018: 1-9), aunque, en contra de la transparencia, tampoco consta en la política de privacidad de Airbnb.

²³ Puede consultarse la noticia a través del siguiente enlace: <https://news.booking.com/es-ar/bookingcom-lanza-un-nuevo-planificador-de-viajes-con-inteligencia-artificial-para-mejorar-la-experiencia-de-organizar-viajes/> [último acceso: 3-9-2024].

²⁴ Puede consultarse la noticia a través del siguiente enlace: <https://tecnohotelnews.com/2023/07/tripadvisor-openai-planificacion-viajes/> [último acceso: 3-9-2024].

²⁵ Véase el apartado «Cookies de marketing» de su política de privacidad. Disponible en: <https://www.booking.com/content/privacy> [último acceso: 3-9-2024].

²⁶ Véase el apartado 3.7.6 de su política de privacidad. Disponible en: <https://www.wimdu.es/aviso-legal#pdp> [último acceso: 3-9-2024].

preferencias a través de la visualización personalizada de publicidad, se conoce como *microtargeting*²⁷.

El empleo de algoritmos de IA debe ponerse en relación con la comunicación digital y conectividad continua, entre sujetos y objetos, que ha posibilitado el IoT, especialmente, tras el notable crecimiento experimentado en los últimos años en el número de dispositivos interconectados. Ciertamente, el IoT ha contribuido a la prestación de servicios mucho más personalizados y específicos por el sector del alojamiento turístico, ya que, como advirtió el extinto Grupo de trabajo del art. 29 (2014a: 4-5), proporciona una infraestructura en la que millones de sensores integrados en dispositivos cotidianos -*smartphones*, relojes inteligentes, vehículos, edificios, etc.- recopilan, procesan, almacenan y transfieren datos personales -dirección IP, coordenadas de geolocalización, *logins* realizados, contraseñas, etc.-, que, al estar asociados a identificadores unívocos, permiten la identificación de individuos, su geoposicionamiento exacto y el seguimiento de sus acciones, conductas y hábitos. Esta cada vez mayor interconexión por redes digitales ha aumentado significativamente la capacidad de generar, comunicar, compartir y acceder a los datos²⁸.

En los últimos tiempos, se ha pensado también en el empleo de tecnología *blockchain* en este campo para proporcionar un registro inmutable, certero y verificable de todas las transacciones realizadas. La *blockchain* o cadena de bloques es una tecnología de registro distribuido (DLT, por sus siglas en inglés) que permite almacenar datos o información de manera segura, transparente e inmutable en una red de carácter descentralizado, es decir, sin necesidad de un organismo que tenga el monopolio sobre el procesamiento y acceso a la información y que verifique las transacciones que en ella se realizan²⁹. Son los propios dispositivos conectados a la red *blockchain*, conocidos como «nodos», los que cotejan, validan y almacenan la información sobre las operaciones celebradas, generando cada uno de ellos una copia completa o parcial de la base de datos, lo que refuerza la seguridad y confianza que proporciona esta red, ya que, al existir numerosas copias de registros, son menos vulnerables a ciberataques o fallos³⁰. La red *blockchain* vendría a ser, pues, una base de datos compartida, donde la información se guarda en unos bloques conectados entre sí mediante una identificación criptográfica, conocida como *hash*, formando una cadena. Cada bloque incluye su propio *hash* y el de su predecesor,

²⁷ Argelich Comelles (2024: 157-158).

²⁸ Al respecto, Tene y Polonetsky (2012: 63-64) y Gutiérrez David (2021:74).

²⁹ Para profundizar sobre el concepto, funcionamiento y tipologías de *blockchain*, véase Luquín Bergareche (2024: 19-34), quien ofrece una aproximación muy práctica sobre esta nueva realidad.

³⁰ World Intellectual Property Organization (2022: 14-16).

lo que certifica que la información -encriptada- no se ha alterado ni se puede alterar³¹.

La tecnología *blockchain* puede ofrecer múltiples ventajas a las plataformas digitales de alojamiento turístico, ya que mejora aspectos claves como la seguridad, la transparencia, la eficiencia y la confianza. Ciertamente, en la medida en que todo dato transaccional está protegido criptográficamente y es inmutable, esta herramienta tecnológica facilita un proceso transparente, inmediato y seguro, lo que impide cargos duplicados, fraudes o cualquier otro tipo de manipulación de la información. Así, todas las operaciones, como los pagos, las reservas o los comentarios de los usuarios, quedan registradas de manera pública, verificable e inmutable en la cadena de bloques, aumentando la confianza de los usuarios en esta información y en la propia red. Además, debe advertirse que, al ser una plataforma descentralizada, se eliminan intermediarios, como las entidades financieras o de gestión de cobro, contribuyendo a que las transacciones sean no solo más transparentes, sino también más económicas.

Son muchas las aplicaciones de interés que presenta dicha tecnología para potenciar la labor de las plataformas de alojamiento turístico. Así, por ejemplo, puede emplearse la criptomoneda como medio de pago o llevarse a cabo la transacción mediante la celebración de *smart contracts* que se ejecutan de forma automática cuando se cumplen las condiciones establecidas. Las características técnicas de esta tecnología disruptiva la convierten también en una herramienta muy óptima para implementar sistemas de reseñas descentralizados, imparciales, transparentes e inmutables, lo que permitiría monitorear de manera más eficaz todas las publicaciones firmadas con la misma clave privada única, garantizando la legitimidad y autoría de la misma al tiempo que aumenta la confianza de los usuarios en esas evaluaciones. También podrían implementarse sistemas de recompensas basados en tokens o criptomonedas, incentivando, de este modo, a los usuarios a publicar comentarios o realizar transacciones.

En la actualidad, encontramos ya algunas plataformas de este sector que emplean tecnología *blockchain*, tales como Travala o Locktrip. Así, la plataforma de alojamiento turístico Travala ha integrado la criptomoneda como medio de pago y ha creado su propio token AVA, ofreciendo un sistema de recompensas que permite a los usuarios obtener descuentos³². Locktrip, por su parte, emplea *smart contracts* que autogestionan la reserva y el pago de los alojamientos, así como la conversión a la criptomoneda propia de la plataforma.

³¹ Organización para la Cooperación y el Desarrollo Económico (2018: 4-6).

³² Consúltase la página web de Travala en el siguiente link: <https://www.travala.com/es/about-us>

Además, permite la tokenización de las habitaciones no utilizadas mediante activos digitales negociables e intercambiables en la red. Cada token representa el derecho a canjear una noche de hotel cuando el portador lo decida³³.

2. IMPACTO DE LAS TECNOLOGÍAS DISRUPTIVAS EN LA PRIVACIDAD Y PROTECCIÓN DE DATOS EN LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO

2.1. EMPLEO DE TECNOLOGÍAS DISRUPTIVAS EN LA RECOPIACIÓN Y TRATAMIENTO MASIVO DE DATOS PERSONALES: APARICIÓN DE NUEVAS CATEGORÍAS DE DATOS Y RIESGOS PARA LA PRIVACIDAD DE LOS USUARIOS

El uso de herramientas tecnológicas disruptivas, como los sistemas de IA de aprendizaje automático o el IoT, han contribuido a la mejora de la productividad y la eficiencia de las plataformas digitales de alojamiento turístico. Estas tecnologías, como hemos visto, permiten la recopilación, procesamiento y análisis de enormes volúmenes de datos, de tal forma que las plataformas pueden detectar patrones de comportamiento, preferencias y necesidades de sus usuarios, y ofrecer, en función de ello, servicios personalizados. Ahora bien, sin perjuicio de estas evidentes ventajas, los tratamientos de datos personales que posibilitan estas avanzadas tecnologías suelen ser, a su vez, altamente intrusivos, por lo que plantean riesgos significativos para la privacidad y la protección de datos de los usuarios, lo que hace necesario establecer salvaguardias para protegerlos frente a posibles abusos.

El Reglamento General de Protección de Datos³⁴ (RGPD) nació, precisamente, para dar respuesta a las necesidades acuciantes de un entorno caracterizado por la digitalización económica y social, donde la vulnerabilidad y la exposición a la que se veían sometidas las personas a través de sus datos personales se hacía cada vez más evidente³⁵. La evolución tecnológica y la globalización, como señalaba en su considerando 6, había supuesto, de un

³³ Consúltase la página web de Locktrip en el siguiente link: <https://locktrip.com/>

³⁴ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

³⁵ Tamayo Velasco (2021: 188) nos recuerda que era un contexto en el que los medios de comunicación comenzaban a visibilizar escándalos en materia de privacidad, como el polémico caso de *Cambridge Analytica* destapado en 2018, y relacionado con el empleo de la minería de datos para

lado, que los individuos difundieran un mayor volumen de información personal, y del otro, que se incrementara de manera significativa la magnitud de la recogida e intercambio de tales datos. Todo ello planteaba nuevos retos para la protección de los datos de carácter personal que la desfasada Directiva 95/46/CE³⁶ era incapaz de abordar. A tal efecto, el RGPD vino a establecer un estándar global en materia de protección de datos para proteger la privacidad de las personas físicas, definiendo, en su art. 4.1, los datos personales como «toda información sobre una persona física identificada o identificable», es decir, toda información que permita determinar la identidad, directa o indirectamente, de una persona física. En esta línea, su articulado recoge una lista abierta de identificadores, donde encontramos aquellos datos identificativos clásicos, como el nombre o el número de identificación, pero también otros que tienen en cuenta la realidad tecnológica, como los identificadores en línea -dirección IP o identificadores de sesión en forma de *cookies*- o los datos de localización.

Pese a contemplar el factor tecnológico, el RGPD no incluye ninguna referencia explícita a los tratamientos de datos personales mediante *Big Data* y algoritmos de IA. Este cuerpo normativo es, no obstante, plenamente aplicable a las nuevas realidades que pudieran surgir derivadas del empleo de tecnologías disruptivas, pues, aunque no se refiera a ellas de forma expresa, sí regula tratamientos específicos asociados a la implementación de estas técnicas analíticas, tales como la elaboración de perfiles y las decisiones individuales automatizadas³⁷. El empleo de soluciones tecnológicas cada vez más avanzadas y sofisticadas podría conllevar, sin embargo, que el RGPD resultara insuficiente para hacer frente a la problemática que plantea la incesante vigilancia a la que estamos sometidas las personas en el entorno digital. Y es que, a medida que aumenta la complejidad y la autonomía de la solución tecnológica en cuestión, las plataformas pueden recopilar mucha más información a través de tratamientos altamente invasivos e invisibles, lo que incrementa las formas de identificación de los usuarios y posibilita la aparición de nuevas categorías de datos personales que se añaden a los datos proporcionados por los usuarios de manera consciente al crear un perfil dentro de la plataforma.

Ciertamente, el desarrollo de la analítica *Big Data*, junto con la evolución del *IoT* y de los sistemas de IA, ha conllevado que ese escenario tradicional

influir en el voto a las elecciones presidenciales estadounidenses de 2016 de millones de usuarios de Facebook.

³⁶ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

³⁷ Así se ha sostenido de manera reiterada en la doctrina científica. Véase, por todos, Aliaga Martínez y Gutiérrez David (2021:8).

en el que las personas proporcionaban sus datos personales conscientemente ya no sea la única forma, y mucho menos la principal, de recopilación de datos personales por parte de las plataformas. En la actualidad, los datos pueden obtenerse de manera automática, mediante el seguimiento de la actividad del usuario en la red o, incluso, pueden generarse nuevos datos por las propias plataformas a través del empleo de técnicas analíticas. La revolución tecnológica nos permite distinguir, de hecho, entre cuatro categorías de datos personales: los datos proporcionados, los observados, los derivados y los inferidos³⁸.

Los «datos proporcionados», como se ha avanzado, comprenden todos aquellos datos facilitados por los individuos de manera consciente para la creación de un perfil dentro de la plataforma³⁹. En el ámbito del alojamiento turístico, ello incluiría datos ordinarios necesarios para utilizar la plataforma, como la información de contacto, cuenta y perfil -nombre, apellidos, número de teléfono, dirección postal, dirección de correo electrónico, fecha de nacimiento, foto de perfil, etc. -, la información sobre la identidad -DNI o pasaporte para verificar la identidad- o la información de pago -datos bancarios-. También se incluyen los contenidos generados por los usuarios cuando publican comentarios o reseñas⁴⁰, rellenan formularios o participan en encuestas, entre otros⁴¹. Se trata, con carácter general, de datos personales ordinarios que las plataformas digitales podrán tratar de manera lícita siempre que concurra alguna de las bases de legitimación establecidas en el art. 6 RGPD⁴². En el ámbito del alojamiento

³⁸ La clasificación aquí seguida fue desarrollada por Abrams (2014: 1-11), en nombre de The Information Accountability Foundation, y fue acogida, posteriormente, por el Information Commissioner's Office (2017: 12-13).

³⁹ Gautrais (2018: 115-147).

⁴⁰ Recordemos que, según el Information Commissioner's Office (2022a: 35), las opiniones pueden constituir datos personales cuando están vinculadas a una persona identificada o identificable, lo que ocurre con bastante frecuencia en las plataformas de alojamiento turístico.

⁴¹ Véase, en este sentido, la política de privacidad de Airbnb, la cual ofrece una clasificación bastante estructurada y clarificadora sobre los datos proporcionados, distinguiendo, al efecto, entre los datos personales necesarios para utilizar la plataforma y los datos que el usuario proporciona voluntariamente. Mucho menos exhaustivas son las políticas de privacidad de Vrbo o Expedia, que se limitan a advertir que recogen información que los usuarios les proporcionan cuando crean una cuenta, se registran para recibir una oferta o efectúan una reserva. De manera algo dispersa, también alude a los datos proporcionados la política de privacidad de Tripadvisor, a los que denomina información biográfica, entendiendo por tal el nombre, el número de teléfono, la dirección postal y de facturación, el correo electrónico y otra información que el usuario haya revelado voluntariamente. En la misma dirección, la política de privacidad de Booking alude, de manera general, a esa información básica que proporciona el usuario para realizar una reserva -el nombre, los datos de contacto, los nombres de las otras personas con las que viaja, los datos de pago, etc.-, así como a toda aquella información que obtiene la plataforma de las comunicaciones que el usuario realiza a través de ella y de sus comentarios sobre las experiencias.

⁴² Estas bases de legitimación son: 1) el consentimiento del interesado; 2) la ejecución de un contrato o la aplicación de medidas precontractuales; 3) el cumplimiento de una obligación legal;

turístico, tres de estas bases adquieren una relevancia particular: el consentimiento del interesado, la ejecución de un contrato o la aplicación de medidas precontractuales, y la satisfacción de un interés legítimo.

Ahora bien, además de datos ordinarios, algunas plataformas de alojamiento turístico también solicitan a sus usuarios «categorías especiales de datos», es decir, datos que revelan el origen étnico o racial, las opiniones políticas, las creencias religiosas o filosóficas, o la afiliación sindical, datos relativos a la salud o a la vida sexual y la orientación sexual, o datos biométricos. Este es el caso de Tripadvisor, el cual admite recopilar datos sobre la raza, el origen étnico, la orientación sexual o la religión⁴³. También de Airbnb, cuya política de privacidad indica expresamente que el usuario podrá incluir información sobre su salud cuando lo estime oportuno (1.2.4), que recabará información biométrica, como datos de reconocimiento facial obtenidos a partir de fotografías y documentos de identidad, con el consentimiento del usuario (1.2.3), o que puede recibir de terceros información sanitaria, incluida la relacionada con enfermedades contagiosas (1.4.9)⁴⁴. Algunas plataformas que operan con tecnología *blockchain*, como Locktrip, y a los efectos de evitar el blanqueo de capitales y la financiación del terrorismo mediante el empleo de criptomonedas, recopilan también opiniones políticas de sus usuarios⁴⁵.

Debido a la sensibilidad de este tipo de información, el tratamiento de las categorías especiales de datos personales está regulado de manera mucho más estricta por el RGPD y exige seguir una serie de cautelas y garantías recogidas en el art. 9.1. En virtud de este precepto, se prohíbe el tratamiento de esta categoría de datos, salvo que concurriera alguna de las circunstancias del art. 9.2 -excepciones a la prohibición de tratamiento-, a saber, el consentimiento explícito⁴⁶, la

4) la protección de intereses vitales del interesado; 5) el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos, y 6) la satisfacción de un interés legítimo.

⁴³ Véase el apartado «¿Qué categorías de información personal recopilamos y por qué?» de su política de privacidad. Disponible en: <https://tripadvisor.mediaroom.com/es-privacy-policy> [último acceso: 3-9-2024].

⁴⁴ Véase su política de privacidad. Disponible en: <https://www.airbnb.es/help/article/2855> [último acceso: 3-9-2024].

⁴⁵ Véase el apartado «Special Categories of Data» de su política de privacidad. Disponible en: <https://locktrip.com/privacy> [último acceso: 3-9-2024].

⁴⁶ Como advierte Castillo Parrilla (2024: 285), existen dos diferencias entre el consentimiento como base legitimadora *ex art.* 6 y el consentimiento como excepción a la prohibición de tratamiento *ex art.* 9.2: este último tiene que ser explícito y se permite a los Estados miembros desarrollar normas para restringirlo. En el caso de España, el art. 9.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) ha establecido que el solo consentimiento del afectado no será suficiente para tratar datos relativos a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, de manera que será necesario contar con la concurrencia de una segunda excepción *ex art.* 9.2 RGPD.

protección de intereses vitales, datos hechos manifiestamente públicos por el interesado, razones de interés público esencial, etc.

A los «datos proporcionados» se suman los «datos observados», que son aquellos que las plataformas obtienen automáticamente a partir de la huella digital que deja la actividad de un usuario en la red⁴⁷. Esta categoría incluye, entre otros datos personales, la ubicación del usuario obtenida a través de aplicaciones móviles o sensores integrados en dispositivos IoT, los metadatos de las comunicaciones entre usuarios que participan en transacciones en la plataforma, así como la dirección IP y los datos de navegación e interacción con sitios webs y contenidos recopilados a través de herramientas analíticas, como *cookies*, *fingerprinting* y otras técnicas similares⁴⁸. La recopilación de estos datos está estrechamente vinculada al desarrollo y evolución del IoT, ya que se trata de datos registrados a través de dispositivos, sensores o rastreadores, lo que explica que, en los últimos años, y de forma consustancial a la conectividad continua que viene garantizando esta tecnología, se haya producido un aumento significativo en el volumen de información que se recaba de los usuarios por esta vía.

En el concreto ámbito del alojamiento turístico, es habitual que las plataformas recopilen información de geolocalización, así como información de uso de la plataforma -búsquedas, reservas realizadas, fechas y horas de acceso, páginas con las que se ha interactuado, etc.- e información del dispositivo a través del que el usuario accede a la misma -dirección IP, información sobre el dispositivo y su actividad, identificadores únicos, confirmaciones de lectura, etc.-⁴⁹. Esta información generalmente se recaba mediante la instalación de *cookies* y otras tecnologías similares⁵⁰, que requiere el consentimiento libre, específico, informado e inequívoco del usuario, el cual puede emitirse a través de una declaración afirmativa -consentimiento expreso- o de una clara acción

⁴⁷ Abrams (2014: 6).

⁴⁸ Gutiérrez David (2021: 78).

⁴⁹ Puede constatarse en la política de privacidad de Airbnb.

⁵⁰ En las políticas de *cookies* y de privacidad de las distintas plataformas del sector se informa sobre ello. Así, por ejemplo, Booking advierte sobre el uso de *cookies* funcionales, analíticas y de marketing, que pueden ser propias o de terceros, así como de tecnologías de seguimiento muy similares, como balizas web, *scripts*, URL de seguimiento o kits de desarrollo de *software* (SDK). Junto a ello, la plataforma utiliza técnicas, como los píxeles de e-mail, que no almacenan información en el dispositivo. Vrbo y Expedia, por su parte, emplean *cookies* esenciales, de funcionalidad, de rendimiento y de segmentación, así como otras tecnologías similares, como contadores de visitas, *GIF*, *GIF* transparentes, balizas de proximidad, píxeles, etiquetas, *scripts* u objetos de almacenamiento local. La plataforma Airbnb, además de utilizar *cookies* de sesión y *cookies* persistentes, emplea rastreadores analíticos propios, como *Cookies Flash*, *fingerprinting*, etiquetas de píxeles, balizas web, así como rastreadores de terceros, que incluyen tecnologías de píxeles y *plugins* sociales de Facebook. Las plataformas que operan con *blockchain* también hacen alusión a técnicas analíticas similares. Así, por ejemplo, mientras Locktrip informa sobre el empleo de *cookies* y balizas web, Travalá advierte sobre el uso de *cookies*, *GIF* transparentes y etiquetas de píxeles.

afirmativa -consentimiento tácito- (art. 4. 11 RGPD)⁵¹. Los avisos de *cookies* permiten al usuario tener consciencia de la obtención y tratamiento de los datos observados, sin embargo, en la práctica, la recopilación de buena parte de estos datos suele pasar desapercibida⁵². Debe, además, tenerse en cuenta que, a través del empleo de estas tecnologías de seguimiento, las plataformas digitales de alojamiento turístico pueden recabar categorías especiales de datos con relativa facilidad, por lo que las plataformas habrán de tomar las cautelas previstas en el art. 9.1 RGPD. Piénsese, por ejemplo, en la consulta por un usuario de páginas webs o descarga de aplicaciones destinadas a personas de una religión concreta o una orientación sexual determinada⁵³.

Junto a los «datos proporcionados» y los «datos observados», encontramos los «datos derivados» y los «datos inferidos», dos taxonomías de datos que genera la propia plataforma mediante el análisis de la información recopilada del usuario. Esta característica, es decir, que sean generados por la propia plataforma, adquiere una especial relevancia desde la perspectiva del derecho a la portabilidad de datos del art. 20.1 RGPD, ya que, según la interpretación del Grupo de trabajo del art. 29 (2016: 10-12), este precepto se aplica a los datos que han sido «facilitados» por el usuario, lo que abarcaría tanto los «datos proporcionados» como los «datos observados». No existe, en consecuencia, un derecho a la portabilidad de los «datos derivados» ni de los «datos inferidos», pues estos quedan fuera del ámbito de aplicación del art. 20.1.

Sin perjuicio de estas notas comunes, ambos tipos de datos presentan diferencias, especialmente en lo que respecta a la complejidad de las técnicas empleadas para su obtención. Más en particular, los «datos derivados» serían aquellos generados mediante la combinación de los «datos proporcionados» y los «datos observados» de manera directa y sencilla, es decir, mediante ope-

⁵¹ Como señaló la STJUE, de 1 de octubre de 2019 (TJCE 2019/209), una casilla marcada por defecto no puede considerarse un consentimiento válidamente emitido, ya que no supone un comportamiento activo del usuario. Además, para que pueda considerarse válido, el usuario habrá de recibir información clara y precisa, lo que implica conocer el tiempo de duración de las *cookies* y si terceros tendrán acceso a la información recabada. Para profundizar sobre la problemática que plantea el consentimiento a las *cookies*, se recomienda el estudio de Castillo Parrilla (2020: 123-131). En noviembre de 2019, la Agencia Española de Protección de Datos publicó una *Guía sobre el uso de cookies* para proporcionar orientaciones a los sitios web que faciliten el cumplimiento de las obligaciones establecidas al respecto en el RGPD. Dadas las cuestiones que el uso de cookies ha seguido suscitando, esta guía ha sido actualizada en diversas ocasiones. La última vez, en mayo de 2024, donde, en línea con las directrices del Comité Europeo de Protección de Datos, se establecen las condiciones para la validez del consentimiento en los modelos de “Pay or OK”, es decir, en aquellos que ofrecen al usuario la posibilidad de pagar por el servicio sin *cookies* o aceptar el uso de *cookies* para publicidad personalizada.

⁵² Así lo hace saber Gutiérrez David (2021: 79), señalando que ello ocurre, por ejemplo, cuando se ejecuta una aplicación en el dispositivo del usuario en segundo plano.

⁵³ Advierte sobre ello la STJUE, de 4 de julio de 2023 (TJCE 2023/152), en sus considerandos 71 a 73.

raciones aritméticas relativamente simples que permiten detectar patrones y generar clasificaciones⁵⁴. Estos datos resultan, por tanto, de relaciones directas y observables en un conjunto de datos original, sin necesidad de emplear modelos estadísticos o de probabilidad para su obtención⁵⁵.

Los «datos inferidos», por su parte, se extraen a través de complejos análisis probabilísticos que detectan correlaciones entre conjuntos de datos y obtienen, a partir de ellas, predicciones sobre el comportamiento de los usuarios⁵⁶. Estas predicciones se emplean, posteriormente, para categorizar o perfilar a los usuarios y elaborar recomendaciones personalizadas. La obtención de este tipo de datos, a diferencia de los anteriores, requiere el empleo de tecnologías disruptivas avanzadas, como los sistemas de IA y, en particular, las técnicas de aprendizaje automático o profundo. Dada la complejidad y opacidad de estas técnicas, esta es no solo la categoría de aparición más reciente, sino aquella que mayores conflictos plantea⁵⁷.

En este sentido, es importante señalar que los datos inferidos se basan en meras probabilidades⁵⁸, por lo que pueden contener errores, omisiones y sesgos, en clara contradicción con el art. 5.1 RGPD, que establece que los datos personales deben ser «exactos», y exige, al efecto, la realización de las operaciones oportunas para detectar y gestionar las imprecisiones derivadas de la aplicación de métodos probabilísticos. Cuando tales operaciones no se realizan y las plataformas emplean esos datos inexactos para la elaboración de perfiles, los sesgos y errores podrían verse reforzados, dando lugar a decisiones discriminatorias y perjudiciales para los individuos. Al mismo tiempo, debe tenerse en cuenta que, para la realización de inferencias o predicciones por las plataformas, es habitual el empleo de hábitos de comportamiento del usuario o de variables sensibles, tales como el origen étnico, el sexo, la orientación sexual o las opiniones políticas, lo que aumenta el riesgo de perpetuar prejuicios hacia ciertos grupos. Aún más preocupante para la privacidad de los individuos resulta la capacidad de las técnicas analíticas de aprendizaje automático para inferir datos sensibles sin que el usuario los haya proporcionado, lo que puede llevar a descubrir correlaciones que revelen información

⁵⁴ Abrams (2014: 7-8).

⁵⁵ A dichos datos parece referirse la plataforma Tripadvisor, cuando establece en su política de privacidad que «cualquier información recibida a través de sitios web de terceros se puede combinar con la información que usted proporciona».

⁵⁶ Abrams (2014: 8).

⁵⁷ Las políticas de privacidad de las plataformas de alojamiento turístico, pese a la problemática inherente a los datos inferidos, les prestan escasa atención en su articulado. Solo de manera muy dispersa se alude a esta categoría o a las técnicas analíticas que se emplean para su obtención. Así, por ejemplo, Booking y Wimdu admiten emplear el algoritmo Criteo para mostrar recomendaciones personalizadas o hacer anuncios de *retargeting*.

⁵⁸ Information Commissioner's Office (2017: 13).

sobre la salud, las convicciones políticas, las creencias religiosas o la orientación sexual de las personas⁵⁹. Todo ello entraña un riesgo significativo para los derechos y libertades de los usuarios, ya que podrían perder el control de su propia identidad y verse privados de manera arbitraria del acceso a bienes y servicios, en contra de su derecho a la protección de datos y del principio de no discriminación. Los efectos lesivos sobre sus derechos pueden ser especialmente graves cuando las correlaciones se realizan utilizando datos sensibles, ya que ello supondrá la exposición de las personas a riesgos elevados de discriminación y de atentados contra sus derechos personales y su dignidad.

En los últimos tiempos, se ha dicho que, frente a los sistemas de IA, que exponen los datos y representan un riesgo a la privacidad, la tecnología *blockchain* es una de las herramientas tecnológicas que más contribuye a reforzar la privacidad y la seguridad de los datos personales de los usuarios, ya que los protege frente a ciberataques. Si bien esto es así, debe advertirse que el empleo por las plataformas de esta tecnología no las exime de los riesgos aquí referidos. Las plataformas de alojamiento turístico que emplean tecnología *blockchain* recaban datos personales de sus usuarios de la misma manera que las otras. Muchos de estos datos son, igualmente, de carácter sensible o se basan en un seguimiento del comportamiento del usuario. Además, también se sirven de algoritmos de IA para elaborar perfiles o tomar decisiones. En definitiva, los riesgos para los derechos y libertades siguen existiendo, por lo que la problemática no radica en la tecnología empleada, sino en la adopción de salvaguardias suficientes para atenuar los efectos lesivos.

2.2. LA ELABORACIÓN DE PERFILES Y LA ADOPCIÓN DE DECISIONES AUTOMATIZADAS A TRAVÉS DE SISTEMAS AVANZADOS DE IA

Los riesgos para los derechos y libertades inherentes al empleo de tecnologías disruptivas avanzadas en el tratamiento de datos personales se tratan de mitigar en el RGPD, a través de la específica regulación de la elaboración de perfiles y el derecho a no ser objeto de decisiones automatizadas. Estos son los únicos tratamientos asociados al uso de IA que la norma europea contempla en su articulado y, aunque se superponen, requieren ser diferenciados, pues el legislador europeo ha previsto garantías concretas para cada uno de ellos.

A este respecto, el art. 22 RGPD establece el derecho del interesado «a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en

⁵⁹ Sobre estos riesgos advierte Garriga Domínguez (2023: 139-146).

él o le afecte significativamente de modo similar». El art. 4.4 RGPD define, por su parte, la elaboración de perfiles como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».

Una lectura conjunta de ambos preceptos permite inferir que la elaboración de perfiles a la que el art. 4.4 alude es una subcategoría de tratamiento automatizado, destinada a categorizar y evaluar individuos, y en la que puede existir o no cierta participación humana⁶⁰. La intervención humana en el perfilado no parece descartar la consideración de este tratamiento como elaboración de perfiles, pues el precepto alude, a diferencia del art. 22, a «toda forma de tratamiento automatizado», donde pueden entenderse incluidas desde formas en las que solo intervienen medios tecnológicos hasta otras en las que, si bien predominan estos medios, existe algún tipo de participación humana. El art. 22 quedaría, por su parte, reservado a las decisiones basadas únicamente en el tratamiento automatizado, es decir, a aquellas que representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano. Así, como señala el Grupo de trabajo del art. 29 (2017: 8), las decisiones automatizadas tienen un ámbito de aplicación distinto y pueden solaparse parcialmente con la elaboración de perfiles o derivarse de esta, en la medida en que pueden llevarse a cabo con o sin elaboración de perfiles.

La elaboración de perfiles es un tratamiento de datos personales, frecuentemente realizado por las plataformas de alojamiento turístico, en el que se recopila y analiza información sobre los usuarios con el fin de identificar patrones, características o comportamientos comunes y crear perfiles que ayudan a clasificar a las personas en categorías específicas para realizar predicciones sobre sus intereses, características o comportamiento futuro. Con carácter general, la recopilación y análisis de datos se realiza mediante algoritmos entrenados para identificar asociaciones entre distintos conjuntos de datos, inferir correlaciones entre diversos comportamientos y atributos de los usuarios, y predecir su comportamiento futuro a partir del perfil generado⁶¹. La plataforma Booking advierte sobre este tratamiento en su política de privacidad:

Te clasifican asignándote un perfil de intereses, por ejemplo, en función de las webs que visitas y los clics que haces. Usamos estos perfiles para mostrar contenido personalizado (como ideas de viaje o alojamientos concretos) en Booking.com y en otras webs.

⁶⁰ En el mismo sentido, Sancho Villa (2021: 1730-1732).

⁶¹ Information Commissioner's Office (2018: 4-5).

La potencialidad de la elaboración de perfiles para el sector del alojamiento turístico reside en que permite construir un perfil muy preciso sobre cada usuario y proporcionarle, en función de este, información personalizada, por lo que se trata de un tratamiento típico en el marco de las actividades de mercadotecnia directa y publicidad⁶². Así, mediante diferentes técnicas de marketing, las plataformas personalizan la información que visualiza cada usuario, orientando las decisiones del mismo en función de su perfil extraído o en favor de los intereses de la propia plataforma, lo que podría tener un impacto directo en la libre competencia, la privacidad y la protección de datos⁶³. En este sentido, debe advertirse que muchas de las estrategias de marketing implementadas por las plataformas, como el *microtargeting* conductual, se basan en el tratamiento algorítmico de los datos del usuario para manipular su decisión⁶⁴. El propio diseño de los algoritmos explota las vulnerabilidades de los usuarios y permite un extenso conocimiento sobre sus intereses, gustos, opiniones y estados emocionales, de manera que su elección final se puede inducir con base en orientaciones emocionales, como decisiones impulsivas o irracionales, o sugerencias en los momentos más adecuados, como serían las horas de descanso⁶⁵. Además, estas técnicas están orientadas a sesgar la información, por lo que los productos o servicios dejan de ser accesibles para todos los usuarios, quienes solo pueden visualizar aquellos que el algoritmo ha determinado para ellos⁶⁶. Ello podría conducir a un eventual resultado discriminatorio en la elección del consumidor.

Estas estrategias de marketing escapan al ámbito material de aplicación de la Directiva 2005/29 sobre prácticas comerciales desleales⁶⁷, pues, como ha señalado Argelich Comelles (2024: 158), difícilmente de una sugerencia personalizada puede inferirse una práctica agresiva que implique presión sobre el usuario. El RGPD, de hecho, da cabida expresamente al perfilado con fines de mercadotecnia directa, determinando, al efecto, que el interesado tendrá derecho a oponerse al tratamiento de datos personales en todo momento (art. 21.2). Como en cualquier otro tratamiento de datos personales, y en virtud del principio de transparencia, las plataformas tienen el deber de informar a los interesados, de manera concisa, transparente, inteligible y de fácil acceso, con un

⁶² Pese a ello, solo algunas políticas de privacidad, como la de Vrbo, Booking o Wimdu, contemplan expresamente la elaboración de perfiles para mostrar publicidad segmentada o realizar operaciones de *retargeting*.

⁶³ Lo ha señalado Hacker (2023: 142-175).

⁶⁴ Puede verse un interesante estudio al respecto en Caló (2014: 995-1051).

⁶⁵ Mik (2016: 1-38).

⁶⁶ Ebers (2018: 1-12).

⁶⁷ Directiva 2005/29/CE del Parlamento europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo.

lenguaje claro y sencillo, de los fines del tratamiento y su base jurídica (arts. 12, 13.1.c y 14.1c). Sin embargo, muchas plataformas de alojamiento turístico no hacen constar la base jurídica en sus políticas de privacidad⁶⁸ o no la identifican claramente⁶⁹. En otros casos, la base jurídica invocada es el interés legítimo⁷⁰. A este respecto debe advertirse que, si bien el RGPD autoriza el tratamiento de datos con fines de mercadotecnia directa en base al interés legítimo de la plataforma, esta base legitimadora no puede invocarse cuando el perfilado represente una intrusión importante en la privacidad, esto es, cuando se trate de perfilados complejos y exhaustivos que implican el seguimiento oculto y prolongado de todas las actividades -en línea y fuera de línea- del usuario y la combinación de grandes cantidades de datos⁷¹. En estos supuestos, la base pertinente será el consentimiento del interesado⁷²; consentimiento que habrá de ser explícito cuando la elaboración de perfiles entre en el ámbito de aplicación de art. 22 RGPD, lo cual no resulta descartable en la actualidad, teniendo en cuenta que los tratamientos de datos en estas plataformas se realizan habitualmente mediante el empleo de algoritmos de aprendizaje automático⁷³.

El art. 22 RGPD prohíbe la toma de decisiones individuales automatizadas que produzcan efectos jurídicos en el interesado o le afecten significativamente de modo similar, si bien esta regla general se exceptúa en tres casos: cuando la decisión esté autorizada por la legislación de la Unión Europea o la de los Estados miembros y se establezcan medidas para salvaguardar los derechos y libertades de los interesados; cuando sea necesaria para la celebración o la ejecución del contrato; o cuando se base en el consentimiento explícito. En estos dos últimos supuestos, el párrafo tercero exige que se garantice al interesado, como mínimo, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Por último, en el párrafo cuarto se establece una limitación en razón de la naturaleza de los datos personales, prohibiéndose la adopción de decisiones automatizadas basadas en datos sensibles o especialmente protegidos, salvo que el interesado haya prestado su consentimiento explícito y esta posibilidad no esté prohibida

⁶⁸ Así, por ejemplo, Tripadvisor o Locktrip.

⁶⁹ Este es el caso de Vrbo o Expedia, las cuales recogen las diferentes bases legales de las que se sirven para el tratamiento de datos personales, pero no especifican cuál de ellas es la que fundamenta la publicidad segmentada.

⁷⁰ Así lo señala expresamente Wimdu: «El fundamento jurídico para este tratamiento de datos [publicidad basada en intereses] es el artículo 6, apartado 1, letra f), del RGPD. Este tratamiento de datos de clientes ya existentes con fines publicitarios se considera un interés legítimo».

⁷¹ Grupo de trabajo del art. 29 (2014b: 31).

⁷² Esta es la base que legitima el tratamiento de datos para la publicidad segmentada en las plataformas Booking o Traval. Airbnb, por su parte, se basa tanto en el interés legítimo como el consentimiento.

⁷³ Gallego Higuera y García Rodríguez (2021: 3729) y Gutiérrez David (2021: 89-90).

por la legislación europea o de los Estados miembros o el tratamiento sea necesario por razones de interés público esencial.

A la luz de este precepto, las plataformas de alojamiento turístico ven bastante limitadas sus posibilidades de adoptar decisiones automatizadas por el riesgo que ello supone para los derechos y libertades de los interesados. No obstante, el consentimiento explícito del usuario, obtenido mediante opciones de suscripción habilitadas en las plataformas a través de un botón de aceptación o mediante acuerdos de tipo *clickwrap* y *browsewrap*, abre una amplia posibilidad a la adopción de este tipo de decisiones, presentándose como una fuga a la efectiva protección de los derechos de los usuarios⁷⁴. La mayoría de plataformas, de hecho, prevén la toma de decisiones automatizadas en sus políticas de privacidad, estableciendo que, en caso de que ello produjera efectos que afectaran significativamente a los usuarios, se implementarán las medidas necesarias para salvaguardar sus derechos, entre los que se incluye el derecho a obtener la mediación humana⁷⁵. Tales decisiones automatizadas establecen los índices de prelación de ofertas, proporcionan recomendaciones de alojamientos, muestran ofertas especiales, filtran el contenido que los usuarios suben a la plataforma o clasifican sus valoraciones.

La toma de decisiones automatizadas puede, no obstante, variar en su alcance⁷⁶. Así, en algunos casos, los algoritmos empleados en la toma de decisiones proporcionan unos resultados que forman parte de un proceso más amplio en el que interviene el ser humano para adoptar la decisión final (*«human in the loop»*)⁷⁷. En otros casos, por el contrario, los sistemas de IA están completamente automatizados y las decisiones que toman se adoptan y ejecutan sin intervención ni supervisión humana⁷⁸. Son estos últimos los que caerían bajo el ámbito de aplicación del art. 22 RGPD en caso de que la decisión automatizada, basada o no en un perfil, tenga efectos jurídicos en el

⁷⁴ En la misma dirección, Argelich Comelles (2024: 156).

⁷⁵ Véase, entre otras, las políticas de privacidad de Booking y Tripadvisor. Mucho más exhaustivas y claras son las políticas de Vrbo o Expedia, que detallan, en consonancia con el art. 22 RGPD, las excepciones a este tratamiento y los derechos que se derivan de él en su apartado «Nuestro uso de la inteligencia artificial».

⁷⁶ Information Commissioner's Office (2022b: 7-8).

⁷⁷ Airbnb, por ejemplo, emplea sistemas automatizados en los que existe intervención humana, con finalidades de prevención de fraude, atención al cliente y mejora de la funcionalidad (2.4): «Cuando sea posible, y en la medida de lo razonable, empleamos métodos automatizados. Es posible que, en ocasiones, tengamos que revisar manualmente algunas comunicaciones, por ejemplo, a efectos de investigar actividades fraudulentas y prestar servicios de atención al cliente o para evaluar y mejorar la funcionalidad de tales herramientas automatizadas».

⁷⁸ Sobre este tipo de tratamiento advierten plataformas como Vrbo o Expedia en el apartado «Nuestro uso de la inteligencia artificial»: «La toma de decisiones automatizada puede consistir en la introducción de tus datos personales en un sistema con el objetivo de que la decisión tomada se calcule empleando procesos automáticos».

interesado o le afecte de forma significativa. Así lo ha advertido expresamente el Grupo de trabajo del art. 29 (2017: 23):

El artículo 22, apartado 1, se refiere a las decisiones «basadas únicamente» en el tratamiento automatizado. Esto quiere decir que no hay participación humana en el proceso de decisión.

El responsable del tratamiento no puede obviar las disposiciones del artículo 22 inventándose una participación humana. Por ejemplo, si alguien aplica de forma rutinaria perfiles generados automáticamente a personas sin que ello tenga influencia real alguna en el resultado, esto seguiría siendo una decisión basada únicamente en el tratamiento automatizado.

Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico.

La ausencia de intervención humana significativa se reputa, por tanto, un elemento fundamental que determina la aplicación del régimen más estricto del art. 22 RGPD, lo cual exigiría a la plataforma fundamentar el tratamiento, bien en la celebración o ejecución del contrato, bien en el consentimiento explícito, así como adoptar las garantías previstas para proteger los derechos de los usuarios. Los tratamientos automatizados que se fundamentan en cualquier otra base jurídica, como el interés legítimo, no serían lícitos. Ahora bien, recientemente, el TJUE, en sentencia de 7 de diciembre de 2023 (TJCE 2023\146), ha realizado una interpretación extensiva del art. 22 RGPD que vendría a extender su aplicación también a las decisiones parcial o semiautomatizadas⁷⁹. En virtud de este pronunciamiento, el grado de participación humana en la decisión pierde la relevancia que había adquirido con anterioridad, pues las garantías del art. 22 RGPD serán de aplicación tanto a aquellas decisiones totalmente automatizadas como a aquellas otras que un humano toma con apoyo en los resultados de un sistema de IA.

Una de las problemáticas que encontrábamos con anterioridad a este pronunciamiento era precisamente que las plataformas de alojamiento turístico, en sus políticas de privacidad, adolecían de cierta ambigüedad a la hora de determinar el grado de intervención humana, por lo que resultaba complejo conocer si esa participación humana era significativa y, por tanto, el tratamiento escapaba del ámbito de aplicación del art. 22. Aunque las plataformas continúan sin especificar este aspecto en sus políticas de privacidad⁸⁰, tras el pronunciamiento europeo, el grado concreto de intervención humana ya no

⁷⁹ Sobre esta resolución, realiza un interesante comentario Cotino Hueso (2024).

⁸⁰ Ilustrativa, en este sentido, es la cláusula antecitada de Airbnb, que habla de la posibilidad de revisar manualmente la información, pero no determina si ese grado de participación humana es o no significativo a los efectos del art. 22 RGPD.

resulta relevante a efectos de la aplicación de este precepto, lo que no obsta a que, por razones de transparencia, deban hacerlo constar en sus políticas. La falta de transparencia no se da solo sobre esta cuestión, ya que muchas plataformas tampoco identifican de manera clara la base jurídica que legitima el tratamiento automatizado, las finalidades del mismo o los datos personales concretos que se utilizarán⁸¹.

Esta falta de transparencia habitual por parte de las plataformas de alojamiento turístico es contraria al RGPD, el cual exige que cualquier tratamiento de datos personales, y con independencia de que entre o no en el ámbito de aplicación del art. 22, cuente con una base de legitimación adecuada y respete los principios básicos para todo tratamiento establecidos en el art. 5. Además, como una de las características principales del tratamiento automatizado es su opacidad para las personas, quienes suelen tener dificultades para comprender su funcionamiento, sus aplicaciones y sus consecuencias, el cumplimiento del principio de transparencia resulta capital en este tipo de tratamientos⁸². Por ello, se exige al responsable que, en caso de decisiones automatizadas *ex* art. 22, adopte las medidas necesarias para facilitar al interesado la información oportuna sobre el tratamiento de datos personales, incluida, la «información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento para el interesado» (arts. 13.2 f, 14.2 g y 15.1 h). El reconocimiento del derecho del interesado a recibir esta información específica es fundamental para garantizar no solo las medidas obligatorias del art. 22.3 -derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión-, sino también el derecho del interesado a obtener una explicación de la decisión tomada⁸³.

Ahora bien, la opacidad intrínseca de los modelos algorítmicos puede determinar la imposibilidad de la plataforma -responsable del tratamiento- de explicar la lógica interna del sistema de decisión, en contra del principio de transparencia. Concurren, de hecho, varios factores que dificultan la explicabilidad de la decisión adoptada: en primer lugar, las empresas no son proclives a revelar sus algoritmos, ya que estos constituyen el núcleo de su modelo de negocio, el cual depende en buena medida de la precisión de las

⁸¹ Véanse, a modo de ejemplo, las políticas de privacidad de Booking o Tripadvisor.

⁸² Así lo establece el propio RGPD en su considerando 58: «Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea».

⁸³ Así lo ha advertido el Grupo de trabajo del art. 29 (2017:28). El derecho a la explicación de la decisión tomada es, no obstante, un punto controvertido en la doctrina, donde existen desde posturas completamente contrarias a su existencia en el RGPD (Wachter *et al.*, 2017: 76-99) hasta otras que defienden la misma (Selbst y Powles, 2017: 233-242).

recomendaciones que ofrecen a sus usuarios; a ello se suma que, en la Unión Europea, los algoritmos se enfrentan a una doble exclusión jurídica, pues no se consideran protegibles ni bajo el régimen de propiedad industrial ni bajo el de propiedad intelectual, por lo que la única vía expedita para su protección es la de los secretos comerciales⁸⁴; por otro lado, la complejidad técnica inherente al algoritmo impide una comprensión generalizada de su funcionamiento, máxime en aquellos casos en los que se trata de algoritmos con una gran autonomía decisoria y que funcionan a modo de caja negra («*black box*»), donde resulta imposible trazar un recorrido completo y comprensible para el ser humano entre la introducción de los datos y la adopción de la decisión⁸⁵; pero es que, aún cuando se logra «abrir» la caja negra y acceder a los datos de entrenamiento, el código fuente, los parámetros, etc., la comprensibilidad e inteligibilidad de los resultados no queda garantizada⁸⁶.

Debido a estas dificultades, el RGPD no exige al responsable del tratamiento que ofrezca una compleja explicación matemática del sistema de IA empleado o la revelación de todo el algoritmo, bastando con que le facilite una información general y comprensible sobre el procedimiento para llegar a la decisión. La información proporcionada debe ser lo suficientemente exhaustiva para que el interesado comprenda los motivos de la decisión y debe incluir una descripción de las variables consideradas, la fuente de dicha información, la pertinencia de la decisión, la existencia de mecanismos internos de revisión o auditoría que garanticen la justicia, efectividad e imparcialidad del modelo algorítmico, así como una información de contacto al que pueda acudir el interesado para solicitar la reconsideración de las decisiones denegadas⁸⁷.

En definitiva, si bien el RGPD recoge una serie de exigencias para garantizar la transparencia de los sistemas de toma de decisiones, la opacidad intrínseca del algoritmo dificulta la efectividad del derecho a una información específica sobre la lógica empleada, y muy especialmente en aquellos casos en los que se emplean sistemas de *deep learning*. Como ha subrayado Rebollo

⁸⁴ Para profundizar sobre ello, véase, Castillo Parrilla (2020: 131-135).

⁸⁵ De hecho, como advierten Barredo *et al.* (2020: 100), a medida que aumenta la complejidad del modelo algorítmico, no solo se incrementa su capacidad para generar predicciones o clasificaciones, sino que disminuye la interpretabilidad de sus resultados.

⁸⁶ Una de las críticas habituales a los modelos de caja negra es que el proceso resulta tan opaco que no solo impide comprender la decisión adoptada al sujeto destinatario de la decisión, sino incluso al propio experto que diseñó el sistema. A este respecto, Bathaee (2018: 905). Solar Cayón (2020:149), por su parte, advierte sobre el riesgo de caer en la «falacia de la transparencia», esto es, asumir que el acceso a la caja negra del algoritmo garantiza la explicabilidad de la decisión y la salvaguardia de los derechos de los interesados.

⁸⁷ Estos son los criterios interpretativos establecidos al respecto por el Grupo de trabajo del art. 29 (2018: 27-30).

Delgado (2023: 108), el art. 22 RGPD vendría, pues, a aportar «una solución tangencial a un problema sobrevenido, como es la aplicación de la IA a bases masivas de datos», pero su eficacia es limitada. Así, dicho precepto presenta utilidad en el contexto de la protección de datos personales, pero no puede resolver otros desafíos que se presentan en relación con el uso que se realiza de la IA, como el eventual riesgo de discriminación algorítmica. Resulta, por tanto, necesaria una regulación más específica que aborde la transparencia algorítmica desde la perspectiva de la protección del sujeto.

3. TRANSPARENCIA ALGORÍTMICA Y RESPONSABILIDAD CIVIL EN EL MARCO DE LA INTERMEDIACIÓN DE LAS PLATAFORMAS DE ALOJAMIENTO TURÍSTICO

3.1. DESAFÍOS QUE PLANTEA LA TOMA DE DECISIONES ALGORÍTMICAS Y LA REGULACIÓN EUROPEA EN MATERIA DE IA PARA COMBATIRLOS

En un contexto en el que las plataformas de alojamiento turístico están dominadas por los sistemas de IA automatizados y semiautomatizados, la transparencia algorítmica se erige como una cuestión clave para la protección de los derechos de los sujetos que intervienen en la contratación de un alojamiento. Los tratamientos algorítmicos gobiernan, en la actualidad, los índices de prelación de ofertas de los alojamientos, los sistemas de recomendación, la fijación de precios, la selección de la publicidad que visualiza cada usuario o los sistemas reputacionales, lo que hace incontestable, a nuestro entender, la exigencia a las plataformas de sólidas garantías en materia de transparencia y responsabilidad por los eventuales resultados discriminatorios o lesivos que se pudieran derivar.

Uno de los riesgos más frecuentes en la adopción de decisiones automatizadas con base en la elaboración de perfiles es la presencia de sesgos algorítmicos y el consiguiente efecto lesivo que ello puede tener en el destinatario de la decisión. Existen, de hecho, decisiones que tienen un impacto muy significativo en las circunstancias, comportamiento o elecciones de los interesados y que, incluso, podrían llegar a provocar su exclusión o discriminación. Piénsese, por ejemplo, en una decisión automatizada que deniega una solicitud de crédito en línea, una oportunidad laboral o el acceso a servicios sanitarios. Se trata de decisiones con graves consecuencias -el RGPD habla de «efectos jurídicos o significativamente similares»- para los interesados que caerían bajo el ámbito de aplicación del art. 22 RGPD.

El sector del alojamiento turístico no está exento de este tipo de decisiones. Así, es una práctica bastante común en estas plataformas la fijación dinámica de precios individuales mediante el empleo de algoritmos, de manera que los precios se van modificando automáticamente en función de la interacción de cada usuario con la plataforma, dando lugar a diferencias en el precio de unos y otros usuarios⁸⁸. A nuestro juicio, estas diferencias de precios podrían llegar a tener efectos significativos en los derechos de los usuarios, si unos precios muy elevados impiden que una persona acceda al servicio de alojamiento o, incluso, si el precio que ha de pagar un usuario por un alojamiento es mucho más elevado al que ha de pagar cualquier otro sobre la base de sus características personales, como su origen racial, sexo o condición discapacitada. Las plataformas de este sector, como ya hemos advertido, también emplean con frecuencia publicidad comportamental basada en la elaboración de perfiles, una técnica de marketing que, si bien en principio es legítima, podría tener efectos significativos en los usuarios por la forma en la que se presenta el anuncio o cuando el tratamiento de datos personales resulta excesivamente intrusivo, explota vulnerabilidades de los interesados o modifica sus deseos y preferencias. Los oferentes de los alojamientos también pueden verse afectados significativamente cuando las reseñas o comentarios de los usuarios contienen sesgos, que el algoritmo no es capaz de filtrar y eliminar, y ello determina que el alojamiento aparezca con baja puntuación, no se muestre con frecuencia o descienda a las peores posiciones. Incluso podría ocurrir que fuera el propio algoritmo el que contuviera sesgos y beneficiara a aquellos alojamientos de ciertas zonas o administrados por un determinado perfil de oferente, priorizando a aquellos de un sexo, raza o nivel socioeconómico en particular.

Estos evidentes riesgos derivados de la toma de decisiones algorítmicas en el marco del alojamiento turístico suelen pasar inadvertidos para los usuarios, pues uno de los rasgos definitorios de la discriminación algorítmica es, precisamente, su invisibilidad⁸⁹. En la mayoría de los casos, los usuarios no son conscientes de que están siendo sometidos a decisiones algorítmicas y, si ignoran este hecho, con más razón desconocen si una decisión les genera efectos lesivos o discriminatorios, lo que les impedirá ejercer su derecho a impugnar la decisión *ex. art. 22 RGPD*. Pero aun detectada dicha discriminación, tampoco resulta sencilla su prueba, en la medida en que el demandante habrá de aportar un elemento de comparación, que en este escenario no es fácil de obtener porque implica tanto el acceso al algoritmo -protegido como secreto empresarial y, muchas veces, ininteligible- como el acceso a datos personales

⁸⁸ Sobre esta práctica y sus consecuencias, véase, Calvano *et al.* (2020: 3267-3297).

⁸⁹ Así lo ha puesto de manifiesto la doctrina. Véase, por todo, Eguíluz Castañeira (2020: 337).

de otras personas -protegidos por la normativa en materia de protección de datos personales-. Además, dada la multiplicidad de sujetos que intervienen en las distintas fases o etapas del proceso decisorio de un algoritmo -programadores, entrenadores del algoritmo, vendedores del *software*, plataformas que lo emplean, etc.- resulta especialmente complejo determinar el agente responsable de los daños generados, máxime teniendo en cuenta que las plataformas no están obligadas a revelar el algoritmo, proporcionando acceso al código fuente, que es la única forma que tendría el demandante de identificar al causante del daño⁹⁰.

Precisamente por todos estos problemas, y ante la insuficiencia del RGPD para hacerles frente, todas las propuestas en materia de IA⁹¹ prevén medidas tendentes a garantizar la transparencia y la explicabilidad algorítmica. En este sentido, la Comisión Europea, en su Libro Blanco sobre la inteligencia artificial, de 19 de febrero de 2020⁹², vino a subrayar la importancia de la transparencia, la responsabilidad y la explicabilidad en los sistemas de IA, proponiendo medidas como auditorías, certificaciones y exigencias informativas para garantizar que las decisiones algorítmicas sean comprensibles y justas. Por su parte, la Carta de Derechos Digitales, adoptada el 14 de junio de 2021 por el gobierno español, proclama el derecho a la igualdad y a la no discriminación, incidiendo en la necesidad de garantizar la ausencia de sesgos en los datos y los algoritmos. En la misma dirección, la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, adoptada por la Comisión Europea el 23 de enero de 2023, asume el compromiso de velar por la transparencia, así como de garantizar que los sistemas algorítmicos no contengan sesgos que pudieran ocasionar decisiones discriminatorias, permitiendo la supervisión humana de todo resultado que pudiera afectar a derechos fundamentales. Todas estas medidas se erigen en principios éticos que buscan orientar el desarrollo de una estrategia y un marco regulador sobre la IA respetuoso con los derechos fundamentales.

Buena parte de estas garantías se han recogido en el Reglamento sobre IA, aprobado el 12 de julio 2024⁹³, la primera ley integral en la materia que

⁹⁰ Advierten sobre estos riesgos en la toma de decisiones algorítmicas, Soriano Arnanz (2021:78) y Berenguer Albaladejo (2023: 343).

⁹¹ Dichas propuestas se enmarcan en el contexto de la Estrategia Europea de Inteligencia Artificial de la Comisión Europea, a través de la cual se pretende convertir a la UE en una región de referencia mundial para la IA. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Plan coordinado sobre la inteligencia artificial, adoptado el 7 de diciembre de 2018 [COM(2018) 795 final].

⁹² Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020 [COM (2020) 65 final].

⁹³ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el

tiene por objeto establecer un marco común para gestionar los riesgos que comportan los sistemas de IA. A tal fin, el Reglamento fija «normas armonizadas de transparencia aplicables a determinados sistemas de IA» (art.1.2 d.) y exige a los proveedores que diseñen y desarrollen los sistemas de IA de alto riesgo «de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida» (art. 13). El Reglamento recoge también la necesidad de emplear datos de calidad para el desarrollo de la IA, lo que implica prestar una especial atención a la mitigación de posibles sesgos que pudieran tener repercusiones negativas en los derechos fundamentales o dar lugar a discriminación (considerando 67 y art. 10.3).

El Reglamento, desde la adopción de un enfoque basado en riesgos, adapta el tipo y el contenido de sus normas a la intensidad y el alcance de los riesgos que presenta cada sistema de IA, lo que supone un avance significativo para la protección de los derechos fundamentales de las personas. Ahora bien, este Reglamento no incorpora un marco jurídico completo ni suficiente en relación con los daños causados por los sistemas de IA, especialmente aquellos derivados de la discriminación algorítmica, razón por la que al mismo le acompañan dos propuestas que tratan de completar el régimen en la materia: por un lado, la Propuesta de Directiva sobre responsabilidad en materia de IA⁹⁴, la cual tiene por objeto adaptar ciertos aspectos de la prueba de responsabilidad extracontractual por culpa a los requerimientos de la IA y, por el otro, la Propuesta de Directiva de responsabilidad por productos defectuosos⁹⁵, que viene a reemplazar a la Directiva 85/374/CEE⁹⁶, para adaptar la responsabilidad por productos a las necesidades de regulación de los sistemas de IA y de la economía circular.

Este nuevo paquete normativo, sin embargo, solo de una manera muy residual resultará de aplicación a las plataformas digitales que utilizan sistemas de IA, en la medida en que las mismas están sujetas a una normativa específica que, aunque no tiene por fin regular el fenómeno de la IA, sí incluye disposiciones que afectan al uso que realizan las plataformas de estos sistemas, im-

que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828.

⁹⁴ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, de 28 de septiembre de 2022 [COM (2022) 496 final].

⁹⁵ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, de 28 de septiembre de 2022 [COM (2022) 495 final].

⁹⁶ Directiva del Consejo de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85 /374/CEE), DO L 210/29.

poniéndoles unos deberes de transparencia y un régimen especial de responsabilidad⁹⁷. Dicho marco jurídico está compuesto, en esencia, por la Directiva 2000/31/CE, sobre el comercio electrónico (DCE), traspuesta al Derecho español por la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSI); el Reglamento (UE) 2019/1150, de 20 de junio, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (RE-P2B); el Reglamento (UE) 2022/2065, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (RSD) y, finalmente, el Reglamento (UE) 2022/1925, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital (RMD).

Dado que el fenómeno de las plataformas digitales cuenta ya con su propia regulación, la reciente legislación en materia de IA se remite a ella en su articulado, advirtiendo que este nuevo régimen no modifica el marco jurídico específico que regula el funcionamiento de las plataformas, sino que, en todo caso, viene a complementarlo. A mayor abundamiento, la Propuesta de Directiva sobre responsabilidad en materia de IA afirma en su Exposición de motivos que la propuesta no afecta a las normas establecidos por el RSD, las cuales configuran «un marco integral y plenamente armonizado para las obligaciones de diligencia debida para la toma de decisiones algorítmica por parte de las plataformas en línea, incluida su exención de responsabilidad para los prestadores de servicios intermediarios». El Reglamento de IA, por su parte, establece que cuando los sistemas de IA se integren en las plataformas en línea de muy gran tamaño estarán sujetas al marco de gestión de riesgos del RSD, y el Reglamento de IA solo les será de aplicación cuando surjan riesgos sistémicos significativos no cubiertos por aquel (considerando 118).

3.2. EXIGENCIAS DE TRANSPARENCIA PARA LOS SISTEMAS ALGORÍTMICOS DE RECOMENDACIÓN, CLASIFICACIÓN, SELECCIÓN DE CONTENIDOS Y PUBLICIDAD EN LÍNEA DE LOS PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS

El punto de partida de la regulación del fenómeno de las plataformas digitales fue la creación legal de los «servicios de la sociedad de la información», consolidada a partir de la adopción en el año 2000 de la DCE, que, como se ha avanzado, fue traspuesta a nuestro Derecho por la LSSI. Dentro de este concepto más amplio, se identificó la categoría específica de «servicios in-

⁹⁷ Más que un régimen propio y diferenciado de responsabilidad, coincidimos con Gálvez Criado (2024: 308) en que se trata de un conjunto de normas que vienen a modular nuestro sistema de responsabilidad en un ámbito concreto y respecto a unos sujetos particulares.

termediarios», quienes quedaban sujetos a un principio general de exención de responsabilidad por los contenidos transmitidos, almacenados o alojados. Con ello se pretendía proteger y promocionar los nuevos servicios digitales.

Las reglas básicas establecidas por la DCE se han mantenido en vigor hasta la actualidad. No obstante, en los últimos años, dicha Directiva se ha reputado insuficiente para abordar las nuevas realidades ligadas a la evolución del ecosistema digital y, especialmente, la aparición de las plataformas digitales, lo que ha sido una fuente de constantes conflictos y ha requerido la intervención del TJUE en varias ocasiones. En lo que aquí concierne, el TJUE vino a confirmar que las plataformas digitales, entendidas estas como aquellos prestadores que coordinan la interacción entre terceros mediante tecnologías digitales, ofrecen «servicios de la sociedad de la información» y, más en particular, «servicios intermediarios de alojamiento de datos», lo que las hace acreedoras de la exención de responsabilidad en la prestación de sus servicios⁹⁸. Esta aproximación vino a ampliar el concepto de «alojamiento de datos», dejando atrás esa concepción pasiva del alojamiento⁹⁹, para admitir en dicha categoría el tratamiento automatizado de los datos a través de complejos algoritmos

El creciente uso de tecnologías disruptivas por parte de las plataformas digitales ha llevado a la UE a adoptar un paquete normativo que, aunque mantiene en vigor la DCE, ha supuesto una importante actualización del régimen jurídico de los prestadores de servicios intermediarios, estableciéndose reglas más claras en relación con la exención de responsabilidad, así como exigencias en materia de transparencia.

La primera norma en regular este nuevo ecosistema digital ha sido el RE-P2B, si bien este se centra de manera exclusiva en las relaciones entre profesionales, esto es, y en lo que al objeto de este trabajo se refiere, la plataforma y el usuario profesional que ofrece a través de la misma servicios de alojamiento hotelero o turístico¹⁰⁰. Quedan excluidos de su ámbito de aplicación los ofe-

⁹⁸ Para profundizar sobre esta cuestión y, más en particular, en algunos de estos pronunciamientos, véase Martínez Nadal (2022a: 391-395).

⁹⁹ Como nos recuerda López Richart (2020: 395-396), a finales de los noventa, cuando se concibió el régimen de exención de responsabilidad de los prestadores de servicios de intermediación, la noción de «servicio de alojamiento» quedaba restringida a los servicios de *hosting*, entendiendo por tal el arrendamiento de un espacio en un servicio externo en el que el usuario puede alojar información, como las páginas o sitios web. Debido a la evolución tecnológica experimentada en los últimos años, el TJUE ha extendido este concepto a todos esos servicios característicos de la web 2.0 que se nutren de los contenidos creados por sus propios usuarios.

¹⁰⁰ Según la clasificación que nos ofrece Álvarez Moreno (2024: 54), los usuarios profesionales pueden ser propietarios o gestores de establecimientos hoteleros -hoteles, hostales, etc.-, anfitriones profesionales de viviendas turísticas, gestores que tienen a cargo una cartera de inmuebles -agencias de viajes, agentes de la propiedad, etc.- o, incluso, administradores de fincas que cuentan con autorización para arrendar los inmuebles.

rentes de servicios de alojamiento turístico que actúan como anfitriones particulares. Su principal objetivo es, de hecho, paliar la situación de indefensión en la que se encuentran los usuarios profesionales frente a las plataformas mediante el establecimiento de normas tendentes a garantizar la transparencia y la equidad en el entorno comercial, aunque ello, por extensión, beneficiará también a los consumidores finales. La razón por la que el Reglamento se centra en la protección de los usuarios profesionales radica en que estos, por más que sean empresarios, siempre acaban ocupando una posición de debilidad contractual frente a las plataformas¹⁰¹, debilidad que, en los últimos años, se ha tornado más acuciante debido a la falta de transparencia en los algoritmos que gobiernan los índices de prelación de ofertas y a la escasez de normas tuitivas que los protejan frente a reseñas o comentarios negativos¹⁰².

En este sentido, debe advertirse que la clasificación de un usuario profesional en una determinada plataforma tiene un impacto fundamental en la elección de los consumidores y, por ello, en el éxito de su negocio, ya que cuanta más visibilidad y detectabilidad tenga, más probabilidades tendrá de ser elegido. La clasificación de los oferentes, como señala Álvarez Moreno (2024:71), puede depender de múltiples factores: la puede elaborar la plataforma mediante la aplicación de distintos criterios objetivos, puede ser resultado de las valoraciones de los consumidores o, incluso, estar condicionada por el pago de remuneraciones por parte de los usuarios profesionales para mejorar su puesto. A este respecto, el art. 5 RE-P2B exige a la plataforma que proporcione una descripción actualizada, fácil y públicamente accesible de los parámetros en los que se basa para realizar las clasificaciones -características de los alojamientos, valoración de los usuarios, efecto del aprendizaje automático, etc.-, indicando el peso relativo que tiene cada uno de estos pa-

¹⁰¹ El propio RE-P2B se hace eco, en sus Considerandos 2 a 6, de la importancia que tienen las plataformas digitales para el éxito comercial de las empresas, así como de la situación de vulnerabilidad en la que estas empresas quedan frente a prácticas unilaterales o injustas, el miedo a represalias o la ausencia de mecanismos efectivos para solicitar una reparación. Como bien señala Arroyo Amayuelas (2021: 25), esta importancia reside en que la creciente intermediación de transacciones a través de servicios en línea, impulsada por fuertes efectos de red indirectos basados en datos, hace que los usuarios profesionales dependan cada vez más de estos servicios para llegar a los consumidores. Debido a esa dependencia cada vez mayor, las plataformas cuentan con una superior capacidad de negociación, lo que les permite «actuar unilateralmente de una manera que puede ser injusta y perjudicar a los intereses legítimos de los usuarios profesionales y, de modo indirecto, también a los consumidores de la Unión».

¹⁰² Lo señala Castillo Parrilla (2022: 266 y 276), afirmando expresamente que «resultaba clamoroso el silencio normativo, el desamparo, en que se encontraban y aún se encuentran numerosos empresarios cuando contratan con otros cuya mayor potencia económica los convierte de facto en parte débil de la relación contractual».

rámetros¹⁰³. Se pretende con ello que el usuario profesional pueda comparar las prácticas de diferentes intermediarios y contratar con el que le resulte más conveniente. Además, a efectos de evitar las manipulaciones en las elecciones de los usuarios finales mediante técnicas de marketing o recomendaciones personalizadas, se obliga a la plataforma a hacer mención explícita del pago por parte del usuario profesional para mejorar su posicionamiento. Finalmente, la plataforma tendrá que informar al usuario profesional sobre la alteración sufrida en dicha clasificación o la expulsión de la misma cuando esta circunstancia se deba a la notificación de un tercero.

Pese al bienintencionado intento de aumentar la transparencia y la equidad en el entorno comercial digital, el RE-P2B presenta una serie de carencias y limitaciones que conviene tener en cuenta. Así, por un lado, aunque se exige a la plataforma proporcionar a los usuarios profesionales información sobre el trato diferenciado de los bienes y servicios ofertados (art. 7), no se les obliga a desvelar el algoritmo que determina la clasificación de la oferta y los resultados de las búsquedas que realizan los consumidores, lo que implica un importante riesgo de discriminación algorítmica cuando existen sesgos en estas clasificaciones o en la propia configuración de los algoritmos. El Reglamento es, por tanto, insuficiente para hacer frente a la discriminación algorítmica a la que están expuestos no solo los consumidores, sino también los propios usuarios profesionales que ofertan servicios de alojamiento turístico. A ello se añade el hecho de que el RE-P2B es una norma que ha tenido una escasa incidencia práctica, un cumplimiento bastante limitado y que aún no ha alcanzado todo su potencial¹⁰⁴. Se trata, por tanto, de un primer paso, aunque tímido, para regular el fenómeno de la economía de plataformas.

De hecho, tras su entrada en vigor, se aprobaron dos grandes Reglamentos Europeos, el RSD y el RMD, que inciden de manera muy directa en los deberes de transparencia que han de cumplir las plataformas y establecen sistemas

¹⁰³ A efectos de facilitar el cumplimiento de esta disposición, la Comisión ha elaborado un listado de directrices sobre la transparencia de la clasificación, donde, entre los parámetros principales, se alude a la personalización, el comportamiento de búsqueda, el historial del usuario, los mecanismos de filtrado o el efecto del aprendizaje automático, entre otros. En relación con los parámetros específicos del sector hotelero, se señala la disponibilidad mínima indicada por el establecimiento, los servicios y las comodidades -restaurante, wifi, aparcamiento, gimnasio, etc.-, la calidad del hotel en relación con la calidad anunciada, las políticas del hotel o el propósito del viaje, por citar algunos de ellos. Véase, la Comunicación de la Comisión «Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo», de 8 de diciembre de 2020 (2020/C424/01).

¹⁰⁴ Así se ha puesto de manifiesto en el Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Regiones sobre la primera revisión preliminar de la aplicación del Reglamento (UE) 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, de 19 de septiembre de 2023 [COM (2023) 525 final].

de supervisión por parte de la Comisión Europea de las plataformas de mayor tamaño. Aunque algunos de estos deberes coinciden con los ya regulados por el RE-P2B, existen diferencias significativas en el ámbito de aplicación. Así, el ámbito de aplicación del RSD es mucho más extenso, en cuanto a los sujetos, que el RE-P2B, ya que este se aplica a las relaciones de la plataforma con profesionales y con consumidores. Además, introduce un régimen especial para las plataformas con más de 45 millones de usuarios («plataformas de muy gran tamaño»), a las que les exige obligaciones adicionales que incluyen evaluaciones anuales de amplio alcance de los riesgos derivados de sus servicios en línea¹⁰⁵. Se trata, en definitiva, de una norma destinada a regular la responsabilidad y las obligaciones de los prestadores de servicios digitales con el objetivo de crear un entorno digital más justo, equitativo y transparente para todos los usuarios que operan a través de ella.

Por su parte, el RMD regula las relaciones entre, por un lado, un tipo de plataformas a las que denomina «guardianes de acceso»¹⁰⁶, es decir, grandes plataformas que han acumulado un elevado poder económico y que cumplen los requisitos exigidos en la normativa¹⁰⁷, y, por el otro, los usuarios. Dicho Reglamento exige a los guardianes de acceso unos deberes particulares en materia de transparencia para evitar aquellos desequilibrios que se pueden dar en el ámbito de la negociación, así como prácticas y condiciones injustas para los usuarios profesionales y los usuarios finales de los servicios que esta plataforma ofrece.

¹⁰⁵ Según el listado publicado por la Comisión Europea, en el ámbito turístico solo la plataforma Booking tiene esta consideración. Ahora bien, este listado no es definitivo y se irá actualizando de forma periódica, por lo que otras plataformas podrían adquirir la condición de plataforma de muy gran tamaño con el paso del tiempo.

¹⁰⁶ El 5 de septiembre de 2023 la Comisión designó, como guardianes de acceso, a Apple, Alphabet, Meta, Amazon, Microsoft y ByteDance. En mayo de 2024, sobre la base de una autoevaluación de Booking, la Comisión ha designado también a esta plataforma como guardián de acceso. Esta es la única plataforma del sector turístico, hasta ahora, que tiene esta condición.

¹⁰⁷ Artículo 3. Designación de los guardianes de acceso:

1. Una empresa será designada como guardián de acceso si: a) tiene una gran influencia en el mercado interior; b) presta un servicio básico de plataforma que es una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales, y c) tiene una posición afianzada y duradera, por lo que respecta a sus operaciones, o es previsible que alcance dicha posición en un futuro próximo. 2. Se presumirá que una empresa cumple los respectivos requisitos establecidos en el apartado 1: a) en relación con el apartado 1, letra a), cuando la empresa consiga un volumen de negocios anual en la Unión igual o superior a 7 500 000 000 EUR en cada uno de los tres últimos ejercicios, o cuando su capitalización bursátil media o su valor justo de mercado equivalente ascienda como mínimo a 75 000 000 000 EUR en el último ejercicio, y preste el mismo servicio básico de plataforma en al menos tres Estados miembros; b) en relación con el apartado 1, letra b), cuando proporcione un servicio básico de plataforma que, en el último ejercicio, haya tenido al menos 45 millones mensuales de usuarios finales activos establecidos o situados en la Unión y al menos 10 000 usuarios profesionales activos anuales establecidos en la Unión, identificados y calculados de conformidad con la metodología y los indicadores establecidos en el anexo; c) en relación con el apartado 1, letra c), cuando se hayan alcanzado los umbrales establecidos en la letra b) del presente apartado en cada uno de los últimos tres ejercicios.

A decir verdad, el RE-P2B se ha visto eclipsado por estos dos grandes Reglamentos que establecen exigencias más estrictas de transparencia para las plataformas, especialmente para aquellas que tienen la consideración de plataformas de muy gran tamaño (RSD) o de guardián de acceso (RMD). Ahora bien, y en lo que al sector del alojamiento turístico se refiere, debe advertirse que solo la plataforma Booking se vería interpelada por ambos textos, ya que es la única que cumple con ambas condiciones. Las previsiones del RMD, de hecho, solo le son de aplicación a ella dentro de este sector. En cambio, las del RSD son aplicables a todas las plataformas del sector en sus relaciones tanto con los empresarios como con los consumidores, salvo, claro está, aquellas exigencias adicionales que el texto contempla para las plataformas de muy gran tamaño, las cuales únicamente afectarán a Booking.

Realizadas estas precisiones, conviene analizar la incidencia que tales textos han tenido sobre el RE-P2B, ya sea ampliando el alcance subjetivo de las exigencias por él establecidas, o bien creando nuevos deberes que no fueron previstos por dicha norma. En cuanto a las exigencias ya recogidas en el RE-P2B, encontramos la relativa a la transparencia algorítmica en los sistemas de recomendación, cuestión sobre la que el RSD se manifiesta de modo similar al RE-P2B. A tal efecto, el RSD exige a las plataformas, en su art. 27.1, que informen en sus condiciones generales, empleando un lenguaje claro y comprensible, de los parámetros principales utilizados, así como de cualquier opción a disposición de los destinatarios finales para modificar o influir en dichos parámetros. Si existieran varias opciones disponibles, las plataformas deben, en virtud del art. 27.3, poner a disposición de los destinatarios del servicio una funcionalidad que les permita seleccionar o modificar en cualquier momento su opción preferida. Booking, por su condición de plataforma de muy gran tamaño, está obligada a ofrecer también al menos una opción que no se base en la elaboración de perfiles (art. 38 RSD).

Entre los nuevos deberes en materia de transparencia algorítmica que introducen estos Reglamentos, encontramos obligaciones de diligencia que implican la adopción de medidas correctoras adecuadas en el diseño y funcionamiento de la publicidad, las interfaces en línea o los sistemas de moderación. En lo que a la publicidad respecta, ambos Reglamentos son conscientes de las posibilidades de perfilado individual que ofrece la aplicación de sistemas de IA en este ámbito, ya que, gracias a estas técnicas, los anunciantes pueden mejorar el alcance e impacto de su publicidad al dirigirse a grupos específicos seleccionados o, incluso, a individuos concretos para influir en su conducta. Ello, no obstante, implica un riesgo de discriminación para los usuarios, especialmente cuando se utilizan datos sensibles, así como un riesgo de manipulación cuando se acentúan las vulnerabilidades y emociones negativas de los mismos modificando su conducta. Precisamente para reducir estos riesgos,

el RSD refuerza el principio de transparencia algorítmica en la publicidad y establece la obligación para las plataformas de informar sobre cuándo y en nombre de quién se presenta un anuncio, los parámetros que se han utilizado para decidir la presentación de publicidad específica, así como las posibilidades de cambiar esos parámetros, ofreciendo, en cualquier caso, explicaciones útiles de la lógica empleada en la presentación de publicidad, incluso cuando la misma se basa en la elaboración de perfiles (art. 26.1 y considerando 68). En caso de que dicho anuncio no lo incorpore la plataforma a su interfaz en línea, sino que sean los propios destinatarios del servicio quienes lo hagan, estas deben ofrecerles una funcionalidad para declarar que ese contenido es una comunicación comercial a fin de que el resto de destinatarios puedan identificarlo de manera clara e inequívoca (art. 26.2). Estas medidas responden a la necesidad de aclarar el funcionamiento opaco y, en general, poco comprensible de cómo se lleva a cabo esta publicidad, así como los procesos de focalización y la selección del momento en que se presenta. Además, y dado sus potenciales efectos negativos, el RSD presta una especial atención a la publicidad segmentada diseñada en base a las vulnerabilidades de los usuarios, prohibiendo la elaboración de perfiles basados en categorías de datos sensibles. Junto a estas obligaciones generales, el art. 39 RSD exige a las plataformas de muy gran tamaño una transparencia adicional, ya que tendrán que hacer pública e incluir en un repositorio información relevante sobre cada anuncio. A los guardianes de acceso, los arts. 5.9 y 10 RMD les exigen, además, que proporcionen a los anunciantes o editores, si estos lo requieren, información de índole económica, de manera diaria y gratuita, sobre cada anuncio del anunciante o que conste en el inventario del editor.

En cuanto a las obligaciones de transparencia en el diseño y organización de las interfaces¹⁰⁸, destaca la prohibición del uso de patrones oscuros recogida en el art. 25 RSD. En virtud de este precepto, se prohíbe a las plataformas en línea diseñar, organizar o gestionar sus interfaces de manera engañosa o que manipule a los destinatarios del servicio, así como de forma que distorsione u obstaculice sustancialmente de otro modo la capacidad de estos de tomar decisiones libres e informadas. Esta prohibición se entendía ya una exigencia derivada de los principios de lealtad y transparencia del art. 5.1 a) del RGPD en relación con el tratamiento de los datos personales¹⁰⁹, sin embargo, el legislador europeo ha tenido por bien reforzarla en el RSD. Dado que las interfaces engañosas pueden utilizarse no solo para acceder y tratar de forma ilícita datos personales de los usuarios, sino también para que estos adopten comportamientos que podrían tener consecuencias negativas para ellos, el

¹⁰⁸ Sobre el concepto general de diseño y la necesidad de que en él rija la transparencia, véase Marín Salmerón (2023: 43-67). También, del mismo autor (2021: 105-136).

¹⁰⁹ Agencia Española de Protección de Datos (2020: 20).

RSD prohíbe a todas las plataformas llevar a cabo prácticas que engañen o manipulen a los destinatarios del servicio u obstaculicen su autonomía en la toma de decisiones. Entre las prácticas prohibidas, el considerando 67 destaca las opciones de diseño abusivas que dirigen al destinatario hacia las decisiones que benefician a la plataforma, solicitan de forma reiterada al destinatario que elija una opción cuando ya se ha hecho -especialmente, mediante ventanas emergentes que interfieren en la experiencia del usuario- o hacen que determinadas opciones sean más difíciles o lleven más tiempo que otras.

Las obligaciones de transparencia algorítmica se extienden, asimismo, a las actividades de moderación de contenidos que llevan a cabo las plataformas, las cuales en muchas ocasiones se realizan mediante sistemas automatizados de moderación. En el ámbito del alojamiento turístico, esta actividad de moderación resulta de especial interés en relación con las reseñas y los comentarios que realizan los usuarios acerca de los alojamientos. Las reseñas, como se sabe, tienen un papel fundamental en la industria turística, ya que ayudan a posicionar a los oferentes en la clasificación. En la actualidad, la decisión de contratar un determinado alojamiento está fuertemente condicionada por las reseñas, que crean una falsa apariencia de veracidad en el usuario, de modo que si la plataforma no verifica y contrasta este contenido, se generarían efectos lesivos tanto para el usuario, que emite su consentimiento en base a informaciones falsas y engañosas¹¹⁰, como para los oferentes, que pierden ingresos debido a su mal posicionamiento en la clasificación como consecuencia de puntuaciones falsas. Además de las reseñas y comentarios de los usuarios, la propia información que proporcionan los oferentes sobre las características del alojamiento resulta fundamental para que el usuario acabe decantándose por contratar un determinado alojamiento. Por esta razón, la actividad de moderación, mediante la detección y retirada de información falsa, inexacta o ilegal de los alojamientos, adquiere una notable relevancia para evitar engaños o manipulaciones de los destinatarios del servicio que obstaculizan la autonomía en la toma de sus decisiones. El riesgo de efectos lesivos se incrementa cuando las actividades de moderación de contenidos se realizan mediante sistemas automatizados, ya que estos pueden contener sesgos que les lleven a identificar y eliminar de manera incorrecta contenido ilícito, cuando no lo es, o, por el contrario, que les impidieran detectar contenido que sí tiene ese carácter, como los discursos de odio o la violencia en los comentarios.

¹¹⁰ A este respecto, nos mostramos conforme con aquella doctrina que ha entendido que, cuando la decisión del usuario de contratar pasa por el sistema reputacional controlado por la plataforma, esta debe responder por el daño derivado de una incorrecta conformación del consentimiento del usuario basado en informaciones falsas y engañosas, ya que estaría provocando un vicio del consentimiento en el usuario que podría llegar a tener efectos lesivos en él. Véase, por todos, Cremades García (2021: 247).

Con el fin de evitar tales riesgos, el art. 15 RSD impone a las plataformas una obligación de transparencia informativa sobre su actividad de moderación. En virtud de este precepto, las plataformas habrán de publicar, al menos una vez al año, informes claros y comprensibles sobre cualquier actividad de moderación de contenidos que hayan realizado. En caso de que hayan empleado medios automatizados, deberán hacer constar este hecho, incluyendo una descripción cualitativa, con referencias a los fines concretos del sistema, los indicadores de la precisión y la posible tasa de error, así como las salvaguardias aplicadas. Se trata, en definitiva, de una obligación que pretende garantizar la rendición de cuentas de las plataformas y, más en particular, que estas alerten sobre el empleo de sistemas automatizados de decisión.

3.3. TRATAMIENTO LEGAL DE LA RESPONSABILIDAD DE LAS PLATAFORMAS POR LA MODERACIÓN AUTOMATIZADA DE CONTENIDOS Y EL INCUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA ALGORÍTMICA: RÉGIMEN TRANSITORIO A LA ESPERA DE UNA REGULACIÓN ESPECÍFICA ACERCA DE LA DISCRIMINACIÓN ALGORÍTMICA

Además de las exigencias en materia de transparencia algorítmica, resulta fundamental el examen de la eventual responsabilidad de las plataformas en caso de daños derivados de decisiones automatizadas, especialmente en lo que respecta a la discriminación algorítmica. En este sentido, debe señalarse que, hasta el momento, el legislador europeo no ha abordado de manera específica el tratamiento legal de la responsabilidad de las plataformas por discriminación algorítmica, de manera que debemos remitirnos al régimen de responsabilidad que recoge el RSD. Este, como se sabe, parte de la idea de la exención de responsabilidad de los prestadores de servicios cuando simplemente ocupan una posición técnicamente neutral, automática y pasiva como intermediarios de la información facilitada y transmitida por terceros (art. 6 RSD). A tenor de este precepto, el prestador de servicios no responderá por el contenido ilícito almacenado por sus usuarios cuando no tuviera «conocimiento efectivo» de que es lesivo de los derechos de un tercero o, teniendo conocimiento de esa circunstancia, actuara de forma diligente para suprimir o imposibilitar el acceso al mismo. A tal efecto, las principales vías para obtener conocimiento de una ilicitud son la notificación de una sentencia, la recepción de una notificación por parte de un usuario o un alertador fiable, o la propia investigación del intermediario. En cualquier caso, el prestador de servicios no estará sujeto a una obligación de monitorización o búsqueda de contenido ilícito (art. 8 RSD), aunque sí que tendrá que establecer mecanismos que permitan la notificación en su servicio de la presencia de este contenido (art. 16 RSD).

En la medida en que la plataforma rompa con esa posición de neutralidad tecnológica y realice un control y tratamiento de la información recibida por los usuarios, perderá esa exención y se le podrá exigir responsabilidad por los daños que esa información transmitida ha ocasionado. En este sentido, Álvarez Moreno (2021: 198-199) señala que, si la plataforma se limita a ser un simple agregador de información o anuncios de los oferentes, se beneficiará de esa exención. Sin embargo, si la plataforma establece sus propias reglas de creación de los anuncios, ofrece asistencia en su elaboración mediante servicios propios o realiza modificaciones en los mismos, entonces la plataforma estaría asumiendo un rol activo, y no tecnológicamente neutro, que le podría hacer incurrir en responsabilidad.

Ahora bien, este régimen de exención de responsabilidad ha de ser interpretado correctamente e integrado en nuestro sistema de responsabilidad civil, lo que requiere realizar algunas precisiones: de un lado, debe tenerse en cuenta que el hecho de que una plataforma no pueda acogerse a esta exención por asumir un rol activo no implica que automáticamente incurra en responsabilidad, puesto que ello dependerá de que se den los presupuestos generales de responsabilidad fijados por una norma de nuestro ordenamiento¹¹¹; y, de otro lado, es importante tener presente que esta exención está pensando en la responsabilidad por los daños que la información facilitada y transmitida a través de ella pueda causar, y no en la responsabilidad por su labor de intermediación contractual, de modo que la misma no sería de aplicación en las obligaciones contractuales que asume la plataforma¹¹².

En línea con lo expuesto, la exención de responsabilidad *ex art. 6 RSD* tiene perfecto encaje en el marco de aquellas actividades de moderación automatizada de contenidos que lleva a cabo la plataforma sobre la información que publican sus usuarios -reseñas, comentarios, información de los alojamientos, etc.-, a la cual podrá acogerse siempre que no tenga conocimiento ni control de esa información transmitida o almacenada. En la actualidad, sin embargo, como señala Martínez Nadal (2022a: 394), las plataformas -y, en particular, las de alojamiento turístico- suelen desempeñar un papel activo, incluso de control o influencia decisiva sobre el servicio subyacente, lo que permite, cuanto menos, cuestionar que estas llevan a cabo una intermediación neutra. No lo ha entendido del mismo modo, como se sabe, el TJUE, quien, al pronunciarse

¹¹¹ Tur Faúndez (2021: 1813).

¹¹² Así lo ha señalado Álvarez Moreno (2021: 191). A este respecto advierte Gálvez Criado (2024: 308) que es muy habitual que las plataformas intervengan en el cumplimiento de obligaciones derivadas del contrato de alojamiento en el que no es parte, por ejemplo, gestionando el cobro del precio del alojamiento u ofreciendo una política de reservas y cancelaciones a los establecimientos. La exención de responsabilidad del art. 6 RSD, como es lógico, no operará en estos casos.

por primera vez sobre la naturaleza jurídica de Airbnb¹¹³, descartó que esta ejerciera una posición de control y de influencia decisiva; consideraciones estas que pueden extrapolarse a las otras plataformas del sector y que les abre la posibilidad de acogerse al régimen de exención descrito. Pero, aunque las plataformas de alojamiento turístico adopten una postura tecnológicamente neutra, no siempre podrán beneficiarse de esta exención. No lo pueden hacer en aquellos casos en los que tengan conocimiento efectivo de la presencia de contenido ilícito, como reseñas falsas, inexactas o que vulneren derechos, y no hayan actuado con diligencia para eliminarlas o impedir el acceso de los usuarios a dicho contenido. Además, como se ha mencionado previamente, la pérdida de la exención no implica automáticamente la atribución de responsabilidad a la plataforma. El perjudicado deberá fundamentar dicha responsabilidad conforme a la normativa de su Derecho interno aplicable según el bien jurídico vulnerado o la legislación sectorial que regule la actividad. Esto incluye, entre otros, el régimen general de responsabilidad civil establecido en los artículos 1902 y siguientes del Código Civil, la LOPDH en casos de intromisión ilegítima en los derechos al honor, la intimidad o la propia imagen, el Código Penal cuando la conducta esté tipificada como delito o el Texto Refundido de la Ley de Propiedad Intelectual¹¹⁴ si se vulneran derechos de autor o conexos.

Además de la exención de responsabilidad, como hemos visto, el RSD recoge una serie de obligaciones de diligencia en materia de transparencia para las plataformas. La cuestión que se plantea es si el incumplimiento de estas obligaciones les privaría de la exención de responsabilidad del art. 6. Nada en tal sentido se dice a lo largo de su articulado, más bien al contrario, su considerando 41 señala que las obligaciones de diligencia debida son independientes de la cuestión de la responsabilidad de los prestadores de servicios intermediarios y deben apreciarse por separado¹¹⁵. En todo caso, lo que sí prevé el Reglamento es un derecho específico a obtener una indemnización de los prestadores de servicios por cualquier daño o perjuicio sufrido como consecuencia del incumplimiento por parte de tales prestadores de las obligaciones que el RSD les impone (art. 54). El derecho de indemnización se concede

¹¹³ STJUE, de 19 de diciembre de 2019 (TJCE 2019/302).

¹¹⁴ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

¹¹⁵ Sin perjuicio de ello, como ha señalado De Miguel Asensio (2022:18), es evidente que el incumplimiento de ciertas obligaciones de diligencia -como la de implantar mecanismos de notificación- resultarán relevantes para apreciar que el intermediario, habida cuenta de los riesgos que genera su servicio y de la ausencia de diligencia con la que ha actuado, obtuvo -o debió obtener- conocimiento efectivo de ciertos contenidos ilícitos a los efectos de no poder acogerse a la exención de responsabilidad conforme al art. 6 RSD.

al «destinatario del servicio», entendido este en términos especialmente amplios, lo que incluye no solo a los suscriptores del servicio o a quienes difunden contenidos a través del mismo -quienes eventualmente podrían encontrarse en posición de ejercitar acciones de naturaleza contractual contra la plataforma-, sino también a cualquiera que utiliza la plataforma exponiéndose a la información que se muestra en su interfaz (art. 3 p. y q. RSD). Dicho derecho, advierte De Miguel Asensio (2022: 46), habrá de diferenciarse del que pudieran tener los destinatarios del servicio o los terceros con base en otros sectores del ordenamiento, respecto de los que sí resultarán relevantes las normas sobre responsabilidad de los prestadores de servicios intermediarios.

El RE-P2B, por su parte, recoge sus propios instrumentos jurídicos para garantizar el cumplimiento de sus obligaciones de transparencia. Son solo dos: la nulidad absoluta de las condiciones generales de la contratación que no cumplan las exigencias de transparencia establecidas (art. 3.3) y la imposición a las plataformas de una obligación de poner en marcha un sistema interno de tramitación de reclamaciones, así como de propiciar la mediación como sistema de resolución de conflictos (arts. 12 y 13). Ahora bien, dichos instrumentos, como señala el art. 1.4, se entienden sin perjuicio de los remedios con los que cuente cada Derecho nacional. En el caso del Derecho español, encontramos el régimen sancionador de los arts. 37 y ss. LSSI, las acciones del 32 de Ley de Competencia Desleal¹¹⁶ y el Derecho civil contractual, en especial, la resolución del contrato por incumplimiento del art. 1124 CC y la indemnización de los daños y perjuicios derivados de este incumplimiento del art. 1101 CC.

El paquete digital cuenta, por tanto, con diversos instrumentos para garantizar el cumplimiento de sus exigencias en materia de transparencia algorítmica, sin embargo, no permite resolver todos los problemas jurídicos que plantea el empleo de sistemas automatizados de IA y, especialmente, aquellos vinculados a la responsabilidad por discriminación algorítmica. En este sentido, si bien los deberes de transparencia son fundamentales para descubrir desviaciones en los sistemas de IA que, de otro modo, pasarían desapercibidas, no pueden impedir que los sistemas automatizados lleguen a resultados sesgados y/o discriminatorios. Para ello, hubiera sido necesario que estos mecanismos de prevención de la discriminación algorítmica se vieran acompañados de la articulación de medidas efectivas reparadoras de la misma. Sin embargo, lejos de ello, el paquete digital permite a las plataformas acogerse al régimen de exención del art. 6 RSD siempre que no tuvieran «conocimiento efectivo» del contenido ilícito, lo que les permite exonerarse de eventuales reclamaciones de responsabilidad por los efectos lesivos o discriminatorios que se pudieran

¹¹⁶ Ley 3/1991, de 10 de enero, de Competencia Desleal.

derivan del empleo de sistemas automatizados sesgados. Las plataformas pueden, incluso, acogerse a esta exención cuando han incumplido alguna de sus obligaciones en materia de transparencia algorítmica, ya que el RSD no prevé una vinculación entre el incumplimiento de esas normas y la privación de la exención de responsabilidad. Además, si bien el art. 54 RSD reconoce el derecho a la indemnización de los daños y perjuicios del destinatario del servicio cuando la plataforma ha incumplido una de sus obligaciones -lo que debe juzgarse de manera muy positiva-, el parco contenido de este precepto y las limitaciones del Derecho de la UE en este ámbito determinan que en su aplicación práctica pueda plantear complejos problemas de interpretación, especialmente en paralelo con otras normas, como el art. 82 RGPD¹¹⁷, que recoge el mismo derecho para los perjudicados por la normativa de protección de datos personales. Como ilustra la STJUE, de 4 de mayo de 2023 (TJCE 2023\79), relativa el derecho a la indemnización del art. 82 RGPD, no toda infracción del RGPD generará, por sí sola, un derecho a ser resarcido, quedando supeditado este a la existencia de un nexo causal entre la infracción cometida y el perjuicio ocasionado por la misma. Se trata este, como han declarado expresamente las SSTJUE de 21 de diciembre de 2023 (JUR\2023\449592) y de 11 de abril de 2024 (JUR\2024\106581), de un régimen de responsabilidad por culpa, la cual se presume, a menos que el responsable del tratamiento demuestre que los daños y perjuicios en modo alguno se deben a su culpa o negligencia. Mismas consideraciones podemos entender trasladables al art. 54 RSD, por la similitud que presenta con el art. 82 RGPD, de tal forma que el perjudicado, si bien no ha de probar la culpa de la plataforma, sí tiene que demostrar la conexión causal existente entre la falta de transparencia y el daño padecido, circunstancias que lo siguen enfrentando a la elevada dificultad de la identificación y prueba de la discriminación algorítmica. Parece poco factible, pues, que los efectos lesivos derivados del empleo de sistemas algorítmicos puedan resolverse por esta vía.

Con todo, debe advertirse que el régimen previsto por el paquete digital será revisado y agravado por el Grupo de Expertos para el Observatorio de la Unión Europea sobre la economía de las plataformas en línea debido a la insuficiencia del régimen sancionador y la escasa aplicación que ha tenido el RE-P2B. Ya en 2019, el *European Law Institute* elaboró una propuesta para regular las plataformas en línea¹¹⁸, apostando por una responsabilidad más agravada que hasta ahora ha sido desatendida. En la misma dirección, destacada doctrina europea¹¹⁹ ha advertido que, dadas las causas de exoneración

¹¹⁷ Lo ha advertido también, De Miguel Asensio (2022: 47).

¹¹⁸ European Law Institute (2019: 1-65).

¹¹⁹ Frosio (2017:19-46), Cauffman (2021) y Büyüksagis (2022: 64-86). Recientemente, también lo ha sostenido en nuestro país, Argelich Comelles (2023:135).

recogidas en el RSD y la insuficiencia de las obligaciones de diligencia del RE-P2B, el actual régimen no permite abordar la discriminación algorítmica, para lo que será necesario un régimen agravado tendente a la responsabilidad objetiva, en términos de *strict liability* o *semi-strict liability*, tal y como se contiene en el informe del Parlamento Europeo *Liability of Online Platforms*, publicado el 5 de febrero de 2021¹²⁰. El régimen actual, por tanto, podría constituir, un tratamiento legal transitorio a la espera de una regulación específica acerca de la discriminación algorítmica en este ámbito y la necesaria protección de los sujetos que contratan a través de estas plataformas.

BIBLIOGRAFÍA

- Abrams, M. (2014). *The origins of personal data and its implications for governance*, 1-11. Disponible en: <https://doi.org/10.2139/ssrn.2510927>
- Agencia Española de Protección de Datos (2020). *Guía de Protección de Datos por Defecto*. Madrid: AEPD. Disponible en: <https://tinyurl.com/ywzshtbu>
- Alfaro Águila-Real, J. (2 de mayo de 2016). La regulación de las plataformas. *Almacén de Derecho*. Disponible en: <https://tinyurl.com/26k7pw9p>
- Aliaga Martínez, L. y Gutiérrez David, M.E. (2021). Reino Unido: Tratamientos de datos personales mediante Inteligencia Artificial. Explicando Machine Learning a través de la doctrina y práctica del Information Commissioner's Office. *La Ley Privacidad*, (8), 1-21.
- Álvarez Moreno, M.T. (2021). *La contratación electrónica mediante plataformas en línea: Modelo negocial (B2C), régimen jurídico y protección de los contratantes (proveedores y consumidores)*. Madrid: Reus.
- Álvarez Moreno, M.T. (2024). La reserva de alojamientos en establecimientos hoteleros mediante plataformas digitales. En K. J. Albiez Dohrmann y J. A. Castillo Parilla (dirs.). *Equidad y transparencia en plataformas de alojamiento hotelero en España* (pp. 51-80). Barcelona: Atelier.
- Argelich Comelles, C. (2023). Deberes de transparencia del Reglamento 2019/1150 (P2B Regulation) para prevenir la discriminación algorítmica del consumidor en los sistemas de prelación de ofertas. *Cuadernos de Derecho Transnacional*, 15(1), 129-135. Disponible en: <https://doi.org/10.20318/cdt.2023.7535>
- Argelich Comelles, C. (2024). Transparencia de las plataformas de alojamiento hotelero como causa de exoneración de responsabilidad y PropTech para los hoteles 4.0. En K. J. Albiez Dohrmann y J. A. Castillo Parilla (dirs.). *Equidad y transparencia en plataformas de alojamiento hotelero en España* (pp. 147-172). Barcelona: Atelier.

¹²⁰ Parlamento Europeo (2021).

- Arroyo Amayuelas, E. (2021). El derecho de las plataformas en la Unión Europea. En *Servicios en plataformas: estrategias regulatorias* (pp. 21-69). Madrid: Marcial Pons.
- Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., GARCÍA, S., ... Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. Disponible en: <https://doi.org/10.1016/j.inffus.2019.12.012>
- Barrios Andrés, M. (2020). *Manual de Derecho Digital*. Valencia: Tirant lo Blanch.
- Bathae, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31, 889-938.
- Beltrán Pardo, M. y Sevillano Jaén, F. (2013). *Cloud computing, tecnología y negocio*. Madrid: Paraninfo.
- Berenguer Albaladejo, C. (2023). Efectos discriminatorios de las decisiones adoptadas mediante sistemas de aprendizaje automatizado. En M.C. Bayod López (dir.) y J. L. Argudo Pérez (coord.). *Persona y derecho civil, los retos del siglo XXI (persona, género, transgénero, inteligencia artificial y animales sensibles)* (pp. 335-350). Valencia: Tirant lo Blanch.
- Büyüksagis, E. (2022). Extension of Strict Liability to E-Retailers. *Journal of European Tort Law*, 13 (1) 2022, 64-86.
- Caló, R. (2014). Digital Market Manipulation. *George Washington Law Review*, 82(4), 995-1051. <http://dx.doi.org/10.2139/ssrn.2309703>
- Calvano, E., Calzolari, G., Denicolò, V. y Pastorello, S. (2020). Artificial Intelligence, Algorithmic Pricing, and Collusion. *American Economic Review*, 110(10), 3267–3297. Disponible en: <https://doi.org/10.1257/aer.20190623>
- Castillo Parrilla, J.A. (2020). El turismo en la economía de los datos y la economía de plataformas en la UE. Especial referencia al Reglamento UE 1150/2019. *Revista de Privacidad y Derecho Digital*, (19), 115-155.
- Castillo Parrilla, J.A. (2022). Derechos y garantías concretas del uso de la inteligencia artificial por intermediarios y grandes plataformas. En L. Cotino Hueso (dir.) y M. Bauzá Reilly (coord.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (pp. 259-285). Cizur Menor: Aranzadi.
- Castillo Parrilla, J.A. (2024). Acceso y tratamiento de datos por parte de plataformas y usuarios profesionales de alojamiento hotelero. En K. J. Albiez Dohrmann y J. A. Castillo Parilla (dirs.). *Equidad y transparencia en plataformas de alojamiento hotelero en España* (pp. 271-300). Barcelona: Atelier.
- Cauffman, C. (2019). New EU rules on business-to-consumer and platform-to-business relationships. *Maastricht journal of European and comparative law*, 26(4), 469-479. Disponible en: <https://doi.org/10.1177/1023263X19865835>
- Cotino Hueso, L. (2024). La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección

- de datos y el Reglamento de inteligencia artificial. *Diario La Ley* (80: Sección Ciberderecho). Disponible en: <https://tinyurl.com/yc2bnuxv>
- Cremades García, P. (2021). Contrato de mediación y plataformas digitales de alojamiento turístico. En C. López Sánchez. *El alojamiento colaborativo: problemática jurídica actual de las viviendas de uso turístico* (pp. 221-254). Madrid: Dykinson.
- De Miguel Asensio, P.A. (2022). Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales. *La Ley Unión Europea* (109), 1-47.
- Domínguez Álvarez, J.L. (2024). *Iusalgoritmia: las reglas de derecho y la inteligencia artificial*. Valencia: Tirant lo Blanch.
- Ebers, M. (2018). Beeinflussung und Manipulation von Kunden durch Behavioral Microtargeting. *MultiMedia & Recht*, 1-12.
- Eguíluz Castañeira, J. A. (2020). Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales. *Estudios De Deusto*, 68(2), 325-367. Disponible en: [https://doi.org/10.18543/ed-68\(2\)-2020pp325-367](https://doi.org/10.18543/ed-68(2)-2020pp325-367)
- European Law Institute (2019). Model Rules on Online Platforms. Vienna: ELI. Disponible en: <https://tinyurl.com/bdds4k36>
- Frosio G. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review*, 112, 19-46. Disponible en: <https://tinyurl.com/bdeya2vz>
- Gallego Higuera, G.F. y García Rodríguez, P. (2021). Tratamiento de datos en el ámbito publicitario (Comentario al artículo 23 LOPDGDD). En A. Troncoso Reignada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 3701-3732). Cizur Menor: Aranzadi.
- Gálvez Criado, A. (2024). La responsabilidad civil de las plataformas en línea por el incumplimiento de sus obligaciones legales y/o contractuales en el ámbito del alojamiento hotelero. En K. J. Albiez Dohrmann y J. A. Castillo Parilla (dirs.). *Equidad y transparencia en plataformas de alojamiento hotelero en España* (pp. 301-344). Barcelona: Atelier.
- Garriga Domínguez, A. (2023). Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales. *Revista Española De La Transparencia*, (17 Extra), 137-164. Disponible en: <https://doi.org/10.51915/ret.309>
- Gautrais, V. (2018). The Normative Ecology of Disruptive Technology. In D. Mckee, F. Makela and T. Scassa (eds.). *Law and the «Sharing Economy»: Regulating Online Market Platforms* (pp. 115-147). Ottawa: University of Ottawa Press.
- Gretzel, U., Sigala, M., Xiang, Z. y Koom, C. (2015). Smart tourism: foundations and developments. *Electronic Markets*, 25, 179-188. Disponible en: <https://doi.org/10.1007/s12525-015-0196-8>

- Grupo de trabajo del art. 29 (2014a). *Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos*. (Informe CE. Boletín WP; 223). Bruselas: Comisión Europea. Disponible en: <https://tinyurl.com/2jd2zd64>
- Grupo de trabajo del art. 29 (2014b). *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*. (Informe CE. Boletín WP; 217). Bruselas: Comisión Europea. Disponible en: <https://tinyurl.com/yjb4f4cz>
- Grupo de trabajo del art. 29 (2016). *Directrices sobre el derecho a la portabilidad de los datos*. (Informe CE. Boletín WP; 242 rev.01). Bruselas: Comisión Europea. Disponible en: <https://tinyurl.com/yv4x99e7>
- Grupo de trabajo del art. 29 (2017). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. (Informe CE. Boletín WP; 251 rev-01). Bruselas: Comisión Europea. Disponible en: <https://tinyurl.com/2ux5d87k>
- Gutiérrez David, M. E. (2021). Tratamiento de datos personales *ex machina* en plataformas de turismo colaborativo: concienciación y previsibilidad a través de las políticas de privacidad. *Revista de privacidad y derecho digital*, 6(22), 59-116.
- Hacker, P. (2023). Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal*, 29(1-2), 142-175. Disponible en: <https://doi.org/10.1111/eulj.12389>
- Haldar, M., Abdool, M., Ramanathan, P., Xu, T., Yang, S., Duan, H., ... Legrand, T. (2019). Applying Deep Learning To Airbnb Search. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1-9. Disponible en: <https://doi.org/10.1145/3292500.3330658>
- Hojeghan, S. B. y Esfangareh, A. N. (2011). Digital economy and tourism impacts influences and challenges. *Procedia-Social and Behavioral Sciences*, 19, 308-316. Disponible en: <https://doi.org/10.1016/j.sbspro.2011.05.136>
- Information Commissioner's Office (2017). *Big Data, artificial intelligence, machine learning and data protection*, version 2.2. Disponible en: <https://tinyurl.com/4u3p8fzs>
- Information Commissioner's Office (2018). *Automated decision-making and profiling*, version 1.1.10. Disponible en: <https://tinyurl.com/2s4ybt58>
- Information Commissioner's Office (2022a). *Guide to the General Data Protection Regulation (GDPR)*, version 1.1.17. Disponible en: <https://tinyurl.com/mu5e5sm7>
- Information Commissioner's Office (2022b). *Explaining decisions made with AI*, version 1.03. Disponible en: <https://tinyurl.com/5wtwyc2x>
- Laurent, P., Chollet, T., y Herzberg, E. (2015). *Intelligent automation entering the business world*. Deloitte.
- López Richart, J. (2020). La responsabilidad de las redes sociales y otros prestadores de servicios de alojamiento por los contenidos generados por sus usuarios. En M. J. Herrador Guardia (coord.). *Derecho de daños 2020* (pp. 377-442). Madrid: Francis Lefebvre.

- Luquín Bergareche (2024). *Smart Contracts: aplicaciones jurídicas y de salud digital*. Valencia: Tirant lo Blanch.
- Martínez Nadal, A. (2022a). Naturaleza (y responsabilidad) de las plataformas digitales de la Directiva de Comercio electrónico a la propuesta de Reglamento de Servicios Digitales. En M.J. Blanco Sánchez (coord.), A. Madrid Parra y L. Alvarado Herrera (dirs.). *Derecho digital y nuevas tecnologías* (pp. 387-416). Cizur Menor: Aranzadi.
- Martínez Nadal, A. (2022b). Regulación del arrendamiento turístico en el Derecho español. En A. Martínez Nadal (dir.). *La regulación del alquiler turístico: una aproximación de Derecho comparado* (pp. 57-84). Cizur Menor: Aranzadi.
- Mate Satué, L. C. (2023). La responsabilidad de las plataformas de intermediación contractual en línea: de la Directiva de Comercio Electrónico al Reglamento de Servicios Digitales. En E. Hernández Saínz, L.C. Mate Satué y M.T. Alonso Pérez (dirs.). *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales* (pp. 112-137). A Coruña: Colex.
- Marín Salmerón, A. (2021). El defecto de diseño en la jurisprudencia española: sobre el Risk-utility test y el criterio del diseño alternativo razonable. En J. Ataz López y J.A. Cobacho Gómez (coords.). *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (pp. 105-136). Cizur Menor: Aranzadi.
- Marín Salmerón, A. (2023). *El defecto de diseño en los productos digitales*. Cizur Menor: Aranzadi.
- Más Ferrando, A., Ramón Rodríguez, A.B. y Aranda Cuéllar, P. (2020). La revolución digital en el sector turístico. Oportunidad para el turismo en España. *Ekonomiaz*, (98), 228-251.
- Mik, E. (2016). The erosion of autonomy in online consumer transactions. *Law, Innovation and Technology*, 8(1), 1–38. Disponible en: <https://doi.org/10.1080/17579961.2016.1161893>
- Organización para la Cooperación y el Desarrollo Económico (2018). *OCDE Blockchain Primer*. Paris: OECD Publishing. Disponible en: <https://tinyurl.com/2zuv6zu7>
- Organización para la Cooperación y el Desarrollo Económico (2024). *OECD Tourism Trends and Policies 2024*. Paris: OECD Publishing. Disponible en: <https://doi.org/10.1787/80885d8b-en>
- Pacheco Jiménez, M.N. (2023). Retos jurídicos de las nuevas tendencias en turismo digital. *Revista internacional de Derecho y Economía del turismo*, 5(1), 1-46.
- Parlamento Europeo (2021). *Liability of online platforms*. European Parliamentary Research Service. Disponible en: <https://tinyurl.com/48h6v6tp>
- Ramón Fernández, F. (2022). Inteligencia artificial y su aplicación al turismo. *Revista General de Derecho del Turismo*, (6), 31-78.
- Rebollo Delgado, L. (2023). *Inteligencia artificial y derechos fundamentales*. Dykinson: Madrid.

- Rodríguez de las Heras Ballell, T. (2019). La contratación en plataformas electrónicas en el mercado de la estrategia para un mercado único digital en la Unión Europea. En A. M. Pastor García, I. Martens Jiménez (coords.); P. Castaños Castro, J. A. Castillo Parrilla (dirs.). *El mercado digital en la Unión Europea* (93-127). Reus: Madrid.
- Rodríguez Martínez, I. (2017). El servicio de mediación electrónica y las plataformas de economía colaborativa. *Revista de derecho mercantil*, (205), 181-216.
- Selbst, A. y Powles, J. (2017). Meaningful Information and the Right to Explanation. *International Data Privacy Law*, 7(4), 233-242. Disponible en: <https://doi.org/10.1093/idpl/ix022>
- Sánchez Caparrós, M. (2022). Prevenir y controlar la discriminación algorítmica. *Rubinzal-Culzoni*, 1-34. Disponible en: <https://tinyurl.com/2f7zm3p6>
- Sancho Villa, D. (2021). Las decisiones individuales automatizadas, incluida la elaboración de perfiles (Comentario al artículo 22 RGPD). En A. Troncoso Reignada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales* (pp. 1725-1745). Cizur Menor: Aranzadi.
- Schwab, K. (2016). *La cuarta revolución industrial*. Barcelona: Debate.
- Solar Cayón, J.I. (2020). Inteligencia artificial en la justicia penal: los sistemas algorítmicos de evaluación de riesgos. En Solar Cayón (ed.). *Dimensiones éticas y jurídicas de la inteligencia artificial en el marco del Estado de Derecho* (pp. 125-172). Universidad de Alcalá: Defensor del Pueblo.
- Soriano Arnanz, A. (2021). La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial. En P.R. Bonorino Ramírez, R. Fernández Acevedo y P. Valcárcel Fernández. *Nuevas normatividades: inteligencia artificial, derecho y género* (pp. 63-88). Cizur Menor: Aranzadi.
- Tamayo Velasco, J. (2021). Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada. *Revista de Estudios Europeos*, (78), 183-202.
- Tene, O y Polonetsky, J. (2012). Privacy in the age of Big Data: a time for big decisions. *Stanford Law Review Online*, (63), 63-69.
- Tur Faúndez, M. N. (2021). Responsabilidad civil de las plataformas *on line* en el turismo colaborativo. En J. Ataz López y J.A. Cobacho Gómez (coords.). *Cuestiones clásicas y actuales del Derecho de daños: Estudios en homenaje al profesor Dr. Roca Guillamón* (pp. 1793- 1824). Cizur Menor: Aranzadi.
- Wachter, S., Mittelstadt, B. y Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2) 76-99. Disponible en: <https://doi.org/10.1093/idpl/ix005>
- World Intellectual Property Organization (2022). *Blockchain technologies and IP ecosystems: A WIPO white paper*. Switzerland: WIPO. Disponible en: <https://tinyurl.com/3z5wj5dz>

Implicaciones jurídicas del uso de los robots y la inteligencia artificial en el ámbito sanitario. ¿Hacia una nueva medicina?

ÓSCAR MONJE BALMASEDA

*Profesor Titular de Derecho Civil
(Universidad de Deusto).*

Sumario: 1. LA PROTECCIÓN DE LA SALUD Y LA EVOLUCIÓN TECNOLÓGICA: ESPECIAL REFERENCIA A LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL. 1.1. Consideraciones previas: la robótica y la inteligencia artificial en el ámbito sanitario. 1.2. La utilización de la inteligencia artificial en el ámbito de la salud: sus limitaciones y los desafíos éticos y jurídicos que presenta. 2. PLANTEAMIENTO LEGISLATIVO EN MATERIA DE INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD CIVIL EN LA UNIÓN EUROPEA. 2.1. La responsabilidad civil en el ámbito sanitario. Responsabilidad objetiva y gestión de riesgos. 2.2. El posicionamiento inicial de la Unión Europea en materia de responsabilidad civil de los robots y los sistemas de inteligencia artificial. 2.3. Las propuestas de regulación de la UE: La Directiva sobre responsabilidad por daños causados por productos defectuosos y la Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial.

1. LA PROTECCIÓN DE LA SALUD Y LA EVOLUCIÓN TECNOLÓGICA: ESPECIAL REFERENCIA A LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL

1.1. CONSIDERACIONES PREVIAS: LA ROBÓTICA Y LA INTELIGENCIA AR- TIFICIAL EN EL ÁMBITO SANITARIO

La implantación y utilización generalizada de los avances tecnológicos en el sector de la salud, en materia de prevención, diagnóstico, tratamiento y

seguimiento de las enfermedades ha supuesto sin duda una mayor eficiencia en la toma de decisiones, una notable mejora en la atención sanitaria y en la calidad asistencial, y en lo que ahora interesa destacar, una realidad distinta en torno a la prestación de los servicios de asistencia sanitaria que plantea diversas cuestiones pendientes de respuesta en el ámbito jurídico.

En este contexto de constante innovación tecnológica, nos centraremos en la robótica médica que, como es conocido, está transformando la atención sanitaria al ofrecer soluciones innovadoras que mejoran en gran medida la precisión y la eficiencia de numerosos tratamientos. Se trata, de dispositivos que se utilizan en cirugías y permiten realizar operaciones mucho menos invasivas, con mayor control y menor daño a los tejidos circundantes. Además, los robots desempeñan un papel crucial en la rehabilitación, ayudando a los pacientes a recuperar movilidad a través, por ejemplo, de exoesqueletos y dispositivos de asistencia. En el ámbito del diagnóstico, los robots pueden realizar análisis de imágenes y pruebas con una precisión superior, facilitando diagnósticos más rápidos y exactos, y finalmente, también se utilizan en la logística hospitalaria, gestionando el transporte de suministros y medicamentos, lo que libera al personal médico para que se concentre en la atención al paciente. De este modo, la robótica médica no solo mejora la calidad de la atención, sino que también reduce el tiempo de recuperación de los pacientes, lo que es fundamental en el contexto actual de la salud.

Y a esos avances ya consolidados se suma como objetivos más prometedores en desarrollo, la elaboración de cápsulas médicas inteligentes para llegar al interior del cuerpo humano y abordar un proceso de curación, o las prótesis biónicas avanzadas implantadas directamente en el sistema nervioso central o periférico. La figura simbólica del *cyborg*, entidad en parte orgánica, en parte máquina, se traduce en individuos que, para superar una discapacidad o una enfermedad, pero con la perspectiva de potenciar sus habilidades físicas e intelectuales, afrontan el implante de componentes mecánico-electrónicos en el cuerpo o en el sistema nervioso¹. A través, por ejemplo, de tecnologías ya existentes como la que fusiona el brazo biónico con el cuerpo del usuario mediante osteointegración y lo conecta con el sistema nervioso mediante electrodos implantados en nervios y músculos².

Partiendo de esta realidad, en la actualidad nos encontramos con que el estudio de las implicaciones legales de la robótica en el ámbito sanitario nos conduce necesariamente a la nueva realidad jurídica que se presenta en torno

¹ PALMERINI, E., “Robótica y Derecho, sugerencias, confluencias, evoluciones en el marco de una investigación europea”, en *Revista de Derecho privado*, n° 32, 2017, p. 55.

² <https://es.euronews.com/salud/2023/10/12/un-innovador-brazo-bionico-que-se-fusiona-con-el-esqueleto-y-los-nervios-del-usuario-podri>

a la inteligencia artificial (IA)³, ya que los sistemas de IA pueden consistir en un programa informático o estar incorporados a un aparato físico (robot, dron, vehículo, etc.)⁴.

Precisamente, la inteligencia artificial desempeña un papel crucial en la mejora de la funcionalidad de algunos de estos robots⁵, ya que permite el análisis de grandes volúmenes de datos de cirugías previas, facilitando el aprendizaje y la adaptación a diversas situaciones. Con la IA de lo que se trata es de simular los procesos de la inteligencia humana, incluyendo el aprendizaje el razonamiento y la autocorrección, lo que se hace mediante la creación de algoritmos que funcionan a través de redes neuronales artificiales organizadas por capas, de modo que el conjunto de esas capas forma una red neuronal artificial completa. Con ello, no sólo se imita la inteligencia humana, sino que la supera ampliamente en capacidad de procesamiento de datos y de respuesta.

La IA se utiliza en varias áreas, como el análisis predictivo, que anticipa las necesidades del cirujano durante el procedimiento, y el aprendizaje automático, que mejora el rendimiento del robot a medida que se realizan más cirugías. Además, la asistencia en tiempo real proporciona información y re-

³ De acuerdo con el reciente Reglamento de IA, la definiremos como el “sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales” (artículo 3). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689 En todo caso, sobre el concepto de IA, *vid.* GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Editorial Reus, Madrid, 2023, p. 18 y ss.

⁴ Así se plantea en la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones Inteligencia artificial para Europa. COM/2018/237 final. Document 52018DC0237. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2018%3A237%3AFIN>

Una comunicación en la que también se explica con claridad que el término “inteligencia artificial” (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía- con el fin de alcanzar objetivos específicos.

⁵ En todo caso, refiriéndose al robot Da Vinci, compuesto por una cámara-brazo y un brazo mecánico, que tiene una serie de instrumentos en su extremo, siendo el cirujano quien los controla, aclara ATIENZA NAVARRO, que no obstante su sofisticación, este tipo de sistemas no puede calificarse de inteligencia artificial, y ello porque a pesar de su naturaleza disruptiva e innovadora, no es diferente en el fondo a herramientas menos avanzadas tecnológicamente. Por tanto, sería aplicable la normativa de responsabilidad por productos defectuosos, además de la posible responsabilidad del médico si existiera infracción de la *Lex artis* o, en su caso, al centro sanitario. ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022, pp. 367-368.

comendaciones durante la intervención, lo que contribuye a una mayor eficacia. El proceso de entrenamiento de los robots quirúrgicos con IA implica la recolección de datos de procedimientos anteriores, simulaciones en entornos virtuales que replican condiciones quirúrgicas reales, y el uso de algoritmos de aprendizaje profundo para reconocer patrones y mejorar la precisión.

Es indiscutible, por tanto, que la IA es una tecnología esencial para el desarrollo de la investigación médica y el progreso de los sistemas de diagnóstico y tratamiento de numerosas enfermedades, que ha supuesto un enorme salto cualitativo tanto en el marco de la atención sanitaria como en la práctica clínica diaria, y que presenta posibilidades de futuro que no somos capaces de imaginar⁶.

No es nuestro objetivo describir las últimas innovaciones tecnológicas en el ámbito de la robótica sanitaria, sino destacar y analizar que, además de otras implicaciones jurídicas, esta vertiginosa evolución pone de relieve la importancia de comenzar a sentar las bases relativas a la imputación de los daños que puedan ocasionarse en los procedimientos que requieran su utilización, pues siempre será posible un margen de error, sea de diagnóstico, de procedimiento, de datos incorrectamente administrados, o de transferencia incorrecta⁷.

De hecho, aunque el riesgo cero no sea posible no cabe duda que la prudencia debe ser la pauta en sectores como la protección de la salud, y en este sentido el considerado 47 del recientemente aprobado Reglamento (UE) 2024/1689 sobre Inteligencia Artificial destaca expresamente que “en el sector sanitario, donde puede haber repercusiones especialmente importantes en la vida y la salud, los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, deben ser fiables y precisos”.

1.2. LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO DE LA SALUD: SUS LIMITACIONES Y LOS DESAFÍOS ÉTICOS Y JURÍDICOS QUE PRESENTA

El uso de la inteligencia artificial en el ámbito de la salud está plenamente justificado, al igual que sucede en otros ámbitos socio económicos⁸. Como

⁶ Expone MONTERROSO CASADO, que es muy probable que, a corto plazo, la mayoría de los robots sean programados y que los cirujanos se limiten a supervisar las intervenciones del robot, que será el que efectúe la totalidad o la mayor parte de la misma. MONTERROSO CASADO, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, en MUÑOZ VILLAREAL, A. (Coord.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramientos*, Tirant lo Blanch, Valencia, 2019, p. 105.

⁷ MONTERROSO CASADO, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, *op. cit.*, p. 105.

⁸ Además de aumentar la productividad y la eficiencia, la IA también promete nuevos descubrimientos y ayudar a resolver algunos de los mayores problemas a los que nos enfrentamos:

aplicaciones concretas de la IA en el ámbito de la salud cuya utilidad es innegable nos encontramos con su empleo cada vez más extendido en la prevención y diagnóstico de enfermedades, por ejemplo, en la detección temprana de determinados tipos de cáncer o de cardiopatías ocultas. En efecto, la IA puede analizar grandes cantidades de datos médicos y detectar patrones que podrían pasar desapercibidos para los médicos. Por ejemplo, se utiliza en la interpretación de imágenes médicas como radiografías y resonancias magnéticas para identificar signos tempranos de la enfermedad⁹.

Igualmente, la inteligencia artificial puede ser de gran ayuda en la toma de decisiones y en el tratamiento de enfermedades, como anteriormente destacamos. Su importancia es crucial en el desarrollo de la medicina personalizada ya que IA ayuda a desarrollar tratamientos personalizados basados en el perfil genético y las características individuales de cada paciente. Esto permite una mayor precisión en los tratamientos y una mejor respuesta a las terapias. Y, del mismo modo, los sistemas de IA pueden proporcionar a los médicos información relevante para ayudar en la toma de decisiones sobre el tratamiento de los pacientes lo que incluye recomendaciones sobre medicamentos, procedimientos y cuidados específicos¹⁰.

Por otro lado, en la formación de profesionales sanitarios la IA posibilita la simulación de intervenciones o el entrenamiento de habilidades de diagnóstico, y finalmente no podemos pasar por alto que la investigación médica que en este momento se basa en gran medida en la capacidad de procesamiento de datos e imágenes que posibilita la IA. La IA pueden diseñar nuevos medicamentos desde cero, optimizando las estructuras moleculares para mejorar su eficacia y reducir efectos secundarios. De este modo, se acelera el desarrollo de medicamentos al identificar nuevos compuestos, optimizar ensayos clínicos y permitir reutilizar medicamentos existentes, descubriendo nuevos usos para medicamentos ya aprobados.

desde el tratamiento de enfermedades crónicas, la predicción de brotes de enfermedad o la reducción de las tasas de mortalidad por accidentes de tráfico, hasta la lucha contra el cambio climático o la anticipación de las amenazas a la ciberseguridad. GUTIÉRREZ BARRENENGOA, A.- MONJE BALMASEDA, O., “Algunas aplicaciones concretas de la *robótica* en ámbitos de actuación socioeconómicos. Interactuación posible y, en especial, la responsabilidad civil de los robots”, *Foro galego*, núm. 208, enero-diciembre, A Coruña, 2020, págs. 131 y ss.

⁹ <https://www.apd.es/aplicaciones-inteligencia-artificial-en-medicina/>

¹⁰ En este caso, el problema se suscitará si esa recomendación que propone la inteligencia artificial es errónea, del mismo modo que se plantea ATIENZA NAVARRO que es lo que sucede si se elabora incorrectamente el diagnóstico y/o prescribe un tratamiento erróneo un asistente inteligente, esto es, una aplicación que ayuda a los médicos a adquirir, analizar y elaborar datos clínicos (diagnósticos, tratamientos, etc.), concluyendo con carácter general que no existe negligencia en el profesional que confía en lo indicado por el asistente inteligente, y apostando en cambio por una responsabilidad del hospital. ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, *op. cit.*, pp. 369-370.

Evidentemente, esto no implica que se trata de una tecnología que tiene, y probablemente tendrá durante muchos años importantes limitaciones. El hecho indiscutible de que la IA realice tareas específicas mejor y más rápido que la inteligencia humana, no implica que debamos pronosticar, ni mucho menos admitir, que la IA reemplazará en futuro a los médicos. Desde luego, será de gran ayuda en las especialidades que requieran el análisis de imágenes como, por ejemplo, la radiología y la anatomía patológica. La inteligencia artificial, en la actualidad, acomete con precisión tareas concretas, pero tiene muchas limitaciones en el trabajo completo, ya que aún no es posible la automatización de todas las tareas implicadas en la prestación de la asistencia sanitaria.

Para prescribir un tratamiento médico, o valorar la oportunidad de determinadas intervenciones, hay que considerar y ponderar los datos de las diferentes pruebas que previamente hay que decidir realizar, es preciso además el reconocimiento físico del paciente y de su historial médico que puede presentar lagunas que es necesario aclarar, y estamos lejos de poder automatizar este trabajo. Además, el paciente puede estar exagerando, ocultando o simulando los síntomas de su dolencia, que pueden ser independientes y corresponder a varias enfermedades que concurren simultáneamente en la misma persona. Por tanto, en el diagnóstico y tratamiento posterior de un paciente todo no es capacidad y velocidad de cálculo y procesamiento de datos.

Aunque en el futuro se pudiera automatizar la labor descrita o gran parte de ella, afirma con razón GIL MEMBRADO¹¹ que “el profesional, y por consiguiente, el paciente quedarían abandonados a una suerte de determinismo tecnológico generado por la confianza ciega en la máquina”. En nuestra opinión, no podemos sino seguir apostando por el principio de autonomía supervisada de la máquina lo que implica que la programación inicial y la elección final debe corresponder al humano¹². En el ámbito sanitario no debería poder ser asumible una IA autónoma sin supervisión humana, por lo que el papel idóneo sería servir de sistema de apoyo a la decisión clínica¹³.

¹¹ GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, op. cit., Madrid, 2023, p. 124.

¹² Principio 33 de la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103 (INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

¹³ GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, op. cit., p. 171. Sobre este aspecto concreto, expone acertadamente DIAZ ALABART que, “por mucho que los robots tengan cierta autonomía y puedan tener una aún mayor en el futuro, (...) esa autonomía no procede de que los robots (...) tengan una capacidad volitiva propia. Las capacidades del robot han sido introducidas en él mismo por sus creadores, y su capacidad de aprendizaje obedece a que ha sido programado para ello. No es una cualidad que proceda del mismo. Si bien los robots inteligentes tienen una característica esencial, que es la de ser capaces de aprender, (...) siguen

Pero, si bien la IA y la robótica pueden generar oportunidades también pueden crear un riesgo de perjuicio de intereses jurídicamente protegidos, tanto materiales como inmateriales, por lo que resulta esencial analizar si el actual marco jurídico en materia de seguridad y responsabilidad civil sigue siendo adecuado para proteger a los usuarios y en qué medida¹⁴.

El empleo de la inteligencia artificial en la medicina plantea diferentes desafíos éticos y jurídicos que deben ser considerados y resueltos¹⁵. Uno de los principales es la privacidad de los datos ya que el almacenamiento y empleo de información médica sensible requieren medidas estrictas que garanticen la confidencialidad. Existe, además, el riesgo de sesgos en los algoritmos, que pueden conducir a diagnósticos erróneos si los datos de entrenamiento no son representativos de la población general. La transparencia en cómo se toman las decisiones también es crucial, ya que los pacientes y médicos deben entender cómo y por qué se utilizan ciertas recomendaciones. Otro desafío es la responsabilidad, del que nos ocuparemos específicamente en este trabajo, ya que, en caso de un error es necesario establecer quién o quiénes son los responsables: el cirujano, el fabricante del robot, el programador del sistema de IA, etc. Finalmente, la equidad en el acceso a estas tecnologías es fundamental, ya que no todos los pacientes tienen el mismo acceso a la atención médica avanzada.

Por otro lado, tampoco cabe dudar de la necesidad de adoptar determinadas precauciones frente a los riesgos es esta tecnología. Todas las aplicaciones mencionadas exigen la recogida, almacenamiento y procesamiento de millones de datos que contienen una información muy sensible que forma parte de la vida privada de las personas y que puede ser utilizada con finalidades muy diversas.

siendo cosas (...), si bien la normativa que los regule haya de tomar en cuenta dicha característica". DÍAZ ALABART, S., *Robots y responsabilidad civil*, Editorial Reus, Madrid, 2018, p. 75. En el mismo sentido, BADILLO ARIAS, J.A., "Responsabilidad civil y aseguramiento obligatorio de los robots", en MONTERROSO CASADO, E., (Dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Tirant lo blanch, Valencia, 2019, p. 41.

¹⁴ Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020 (COM (2020) 64 final). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064>

¹⁵ Para NAVARRO MENDIZÁBAL, es tarea nuestra establecer qué es una IA honesta, lo que conllevará prohibir la que no lo sea, la que presente unos riesgos inasumibles por nuestra sociedad y fijar normativa, controles y gestión y limitación de riesgos en los demás casos, a lo que se añade que debemos evitar todo daño de los sistemas con IA y, en el caso de que se produzcan daños, tener un sistema eficaz de reparación y resarcimiento de los daños causados que tendrá que afrontar el responsable para con la víctima. NAVARRO MENDIZÁBAL, I., "¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos", *Revista Iberoamericana de Bioética*, n° 25, 2024, pp. 4-5.

Como explica GIL MEMBRADO¹⁶, pese a sus indudables virtudes, un mayor manejo de la información sanitaria conlleva un mayor riesgo para la protección de la intimidad de la persona, ya que “hay que tener en cuenta que los datos médicos son complejos y no sólo abarcan información estrictamente de salud -que ya de por sí es sensible- sino que además se añade la socioeconómica, la demográfica, los datos de seguros, la dirección postal, la electrónica y los datos que, unidos a la salud, generan una preciosa información sobre nuestra persona”.

Un riesgo que debe ser contemplado en el futuro desarrollo normativo del Espacio Europeo de Datos Sanitarios (EEDS), primer espacio común de datos de la UE en un ámbito específico que surge de la Estrategia Europea de Datos¹⁷, y respecto al que se ha alcanzado, a comienzos de este año 2024, un acuerdo entre el Parlamento Europeo y el Consejo en relación con la propuesta de la Comisión relativa al EEDS¹⁸.

Explica LUQUIN BERGARECHE¹⁹ que, el EEDS pretende configurarse como un ecosistema específico en el ámbito de la salud, formado por reglas, normas y prácticas comunes, infraestructuras y un marco de gobernanza cuyo objetivo es empoderar a las personas para que puedan tener un mayor control y acceso digital a sus datos. Para ello, se apoya su libre circulación, fomentando un auténtico “mercado único” para los sistemas de historiales médicos electrónicos, los productos sanitarios pertinentes y los sistemas de IA calificados “de alto riesgo” por su potencial peligro para la vida y salud (uso primario de los datos). Por otro lado, se pretende alcanzar un marco coherente, fiable y eficiente para el uso de los datos sanitarios en actividades de investigación, innovación, formulación de políticas y reglamentación (uso secundario).

En relación con el tema que nos ocupa, el artículo 37 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios, recogía entre las variadas funciones a desempeñar por los organismos de acceso a los datos sanitarios, la de apoyar el desarrollo de sistemas de inteligencia artificial, el entrenamiento, la prueba y la validación de estos sistemas y el desarrollo de normas y directrices armonizadas en virtud del Reglamento de IA para el entrenamiento, la prueba y la validación de los

¹⁶ GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, *op. cit.*, p.17.

¹⁷ GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, *op. cit.*, pp. 262 y ss.

¹⁸ Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el Espacio Europeo de Datos Sanitarios COM/2022/197 final. Document 52022PC0197. (Disponible en: EUR-Lex - 52022PC0197 - EN - EUR-Lex (europa.eu)).

¹⁹ LUQUIN BERGARECHE, R., “Medicina personalizada y uso secundario de datos de salud para fines de investigación: algunas cuestiones”, *Cuadernos de Derecho Privado*, 8, 2024, pp. 99-100.

sistemas de IA en el ámbito de la salud²⁰. Y, de mismo modo, se obligaba a esos organismos en el artículo 39 a incluir en el informe anual de su actividad, entre otras muchas informaciones, la relativa a la cooperación con otros organismos competentes, en particular en el ámbito de la protección de datos, la ciberseguridad, la cesión altruista de datos y la inteligencia artificial.

Por otra parte, estos avances tecnológicos, así como los inevitables daños ocasionados al utilizarlos, generan una problemática jurídica que no encuentra suficiente y adecuada respuesta en la normativa tradicional de la responsabilidad civil²¹. En efecto, aunque en principio, las normativas en vigor en materia de responsabilidad civil pueden hacer frente con sus recursos a las vicisitudes jurídicas derivadas de las tecnologías emergentes²², la dimensión y el efecto combinado de las dificultades de comprensión y prueba que plantea la IA van a dificultar la indemnización de las víctimas en todos los casos en que esté justificada. Además, estamos, ante una necesidad de orden jurídico que se verá incrementada en los próximos años, ya que en el futuro la problemática se extenderá a muchas de las tareas que actualmente desarrollamos las personas, que serán asumidas por estas tecnologías con un nivel de autonomía respecto a los humanos cada vez mayor²³.

Precisamente por ello, resulta más que justificada la especial importancia prestada a este tema por la Unión Europea. Desde la conocida Resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones desti-

²⁰ En este sentido, conforme al considerando 68 de recientemente aprobado Reglamento de Inteligencia Artificial, “en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a datos sanitarios y el entrenamiento, a partir de esos conjuntos de datos, de algoritmos de IA de una manera segura, oportuna, transparente, fiable y que respete la intimidad, y contando con la debida gobernanza institucional”.

²¹ Sobre este mismo tema, vid. MONJE BALMASEDA, O., “Responsabilidad civil, robótica e inteligencia artificial”, en LLEDÓ YAGÜE, F.; BENÍTEZ ORTÚZAR, I.; et al., (Dir.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, Madrid, 2021, pp. 240 y ss.; MONJE BALMASEDA, O., “Robótica y responsabilidad civil en el ámbito sanitario”, en GIL MEMBRADO, C. (Dir. y Coord.), *Bioderecho y retos. M-Health, Genética, IA, Robótica y criogenización*, Dykinson, Madrid, 2022, pp. 429 y ss.

²² En esta línea, se cuestiona ATIENZA NAVARRO, si hace falta una regulación nueva para los daños causados por la utilización de la inteligencia artificial o basta con alguna de las ya existentes en el ámbito de la responsabilidad civil, con las pertinentes adaptaciones, y concluye, a nuestro juicio con acierto, que puede resultar criticable que se intente dar esa normativa uniforme para un fenómeno tan heterogéneo como la inteligencia artificial, de modo que no sirven fórmulas homogéneas o uniformadoras, sino que deberían tenerse en cuenta sus peculiaridades y los fines o actividad a que se destinan, por lo que resulta conveniente otorgar regulaciones distintas, por ejemplo, en el ámbito de la actividad médica. ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022, pp. 134 y 396-397.

²³ En relación con esta cuestión, vid. DÍAZ ALABART, S., *Robots y responsabilidad civil*, Editorial Reus, Madrid, 2018, p. 75. En el mismo sentido, BADILLO ARIAS, J.A., “Responsabilidad civil y aseguramiento obligatorio de los robots”, *op. cit.*, 2019, p. 41.

nadas a la Comisión sobre normas de Derecho civil sobre robótica²⁴, que se refiere en particular los robots asistenciales, los robots médicos y a la creciente presencia y el potencial de la robótica en la rehabilitación de órganos dañados, el restablecimiento de funciones corporales reducidas y las posibilidades de intervención en el organismo humano, al Reglamento de Inteligencia Artificial de 2024, recientemente aprobado, y demás iniciativas en materia, a las que posteriormente nos referiremos con detalle.

2. PLANTEAMIENTO LEGISLATIVO EN MATERIA DE INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD CIVIL EN LA UNIÓN EUROPEA

2.1. LA RESPONSABILIDAD CIVIL EN EL ÁMBITO SANITARIO. RESPONSABILIDAD OBJETIVA Y GESTIÓN DE RIESGOS

Los robots sanitarios pueden producir daños personales, y también otros de carácter puramente patrimonial, y los daños pueden proceder de algún defecto en la fabricación o programación, de la falta de información sobre su funcionamiento o de la información incorrecta, de la inadecuación del tipo de robot a las tareas que se le han asignado o incluso del uso incorrecto de los mismos por el usuario²⁵. Lo mismo podemos afirmar, con carácter general, de los sistemas de inteligencia artificial utilizados en el ámbito de la protección de la salud.

De este modo, para ofrecer oportuna respuesta en esta materia resulta preciso identificar la causa del daño y el criterio de imputación de responsabilidad aplicable, ya que como explica MONTERROSO CASADO²⁶, no es equiparable un daño como consecuencia de una quemadura durante una intervención a que se deba a un error en el sistema (software). Del mismo modo, será relevante conocer si el daño es consecuencia de la pérdida de control del aparato o de la incorrecta utilización del cirujano o, si lo es por la ausencia de una actualización a una versión superior del sistema, o bien si el resultado se ha producido por una falta de mantenimiento del hospital, un

²⁴ Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103 (INL)). <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017IP0051&from=EN>

²⁵ En este sentido, *vid.* DÍAZ ALABART, S., *Robots y responsabilidad civil*, *op.cit.*, p. 61.

²⁶ MONTERROSO CASADO, E. "Responsabilidad civil por daños causados por robots en el ámbito sanitario", *op. cit.*, 2019, p. 107.

acontecimiento externo (como un ataque informático o una avería en el suministro de energía) o una causa desconocida.

Nos encontramos, en definitiva, con que la problemática planteada es amplia y compleja, y la casuística a resolver ciertamente variada, lo que condiciona el diagnóstico, y conduce a que la solución no pueda ser la misma en todas las situaciones que pueden plantearse.

Aunque lo cierto es que no se trata de opciones excluyentes, en este punto, se presentan como alternativas la responsabilidad objetiva y la gestión de riesgos²⁷. Además, entendemos que en cada ámbito en el que se aplique esta tecnología (transporte, sector sociosanitario, etc.), o persona a la que afecte (menores, personas con discapacidad física o psíquica, etc.), será adecuado uno u otro planteamiento, sin que resulte acertado apostar por una única respuesta.

Para ATIENZA NAVARRO²⁸, que parte de que no es absolutamente prioritario, ni necesario, dar una regulación nueva a los daños causados por los sistemas inteligentes, no hay motivo para instaurar como regla general una responsabilidad objetiva por el mero hecho de que los daños sean causados por la inteligencia artificial, apostando por la determinación del criterio de imputación objetivo o subjetivo según el tipo de sistema inteligente y la actividad en la que se utilice, destacando la importancia del establecimiento de deberes de conducta en los casos de responsabilidad civil subjetiva.

Desde una perspectiva distinta, defiende MONTERROSO CASADO²⁹, que sería oportuno elaborar una ley especial sobre robótica donde se impute la responsabilidad por riesgo al operador y al propietario, de modo similar a como se establece en el R.D.L. 8/2004 de 29 de octubre, en materia de responsabilidad civil y seguro en la circulación de vehículos a motor. No obstante, igualmente coincide este autor en que el régimen de responsabilidad puede coexistir junto con otro sistema de imputación de la responsabilidad si la causación del daño se debe a un uso negligente, por no seguir las instrucciones dadas por el fabricante, un defecto de fabricación o a una falta de actualización. Y del mismo modo, tampoco es incompatible con que se establezcan estándares de calidad y reglas de seguridad que los robots tienen que cumplir y que serían exigibles a los fabricantes del hardware y del software.

²⁷ RUBI PUIG, A., “Retos de la inteligencia artificial y adaptabilidad del derecho de daños”, en Cerdillo I Martínez, A.-Peguera Poch, M. (Coord.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Pamplona, 2020, pp. 68.

²⁸ ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, op. cit., pp. 398, y 406 y ss.

²⁹ MONTERROSO CASADO, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, op. cit., p. 135.

Añade MONTERROSO CASADO³⁰, que el control es uno de los principales criterios de responsabilidad, de modo que deberíamos diferenciar entre la responsabilidad de las tecnologías que podamos controlar (aunque sea de forma indirecta) y que podamos actualizar, por una parte, de las que escapen al control humano y en la actualidad hay que tener en cuenta que los robots en el ámbito sanitario, en general, y en las intervenciones quirúrgicas en particular, no operan de modo totalmente autónoma e independiente, fuera del control humano sino en colaboración con los cirujanos de manera supervisada.

Coincidimos en que a la hora de imputar la responsabilidad es preciso analizar quien supervisa y controla el robot. Sin embargo, concretamente en el ámbito sanitario, tampoco dudamos que el criterio debe ser la responsabilidad objetiva, si el daño procede de la utilización de un sistema de inteligencia artificial.

Se ha destacado, igualmente con razón, que la imprevisibilidad y desconocimiento de los comportamientos de los sistemas inteligentes, está originando una tensión con los fundamentos tradicionales de las reglas de la responsabilidad por daños y con los modos comunes de las cuales el sistema jurídico se viene valiendo para atribuirlos basados en la culpa³¹.

Como argumenta NÚÑEZ ZORRILLA³², enfocando la cuestión desde la perspectiva de la normativa de protección al consumidor, si aplicásemos en el ámbito de la robótica inteligente la misma solución que rige en el sistema tradicional, el fabricante del robot quedaría exonerado de responsabilidad por todos aquellos daños que no hubieran podido ser anticipados; son los que entrarían dentro del margen de la autonomía decisoria del robot. De estos daños debería entonces responsabilizarse al propio robot. Si contrariamente entendemos que el desconocimiento de los posibles daños futuros no puede jugar como eximente entonces deberá responder de ellos mismos el fabricante.

No obstante, sostiene ZURITA MARTÍN³³ que la imprevisibilidad del robot autónomo no es un problema tan difícilmente insalvable, ya que el robot ha de estar diseñado para realizar una serie de actividades o desarrollar ciertas funciones con seguridad, de modo que, si el robot no responde a estas expectativas y causa un daño, estaríamos ante un producto defectuoso por inseguro,

³⁰ MONTERROSO CASADO, E. "Responsabilidad civil por daños causados por robots en el ámbito sanitario", *op. cit.*, pp. 132-133.

³¹ MARTÍNEZ QUIRANTE, R.-RODRIGUEZ ÁLVAREZ, J., *Inteligencia artificial y armas letales autónomas. Un nuevo reto para Naciones Unidas*, TREA, Asturias, 2018, pp. 20 y ss.

³² NÚÑEZ ZORRILLA, M.C. *Inteligencia artificial y responsabilidad civil*, REUS, Madrid, 2018, p. 27.

³³ ZURITA MARTÍN, I. *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Editorial Reus, Madrid, 2020, p. 141.

conclusión que se sitúa en la línea a la que apunta la propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos, que ha sido objeto de aprobación por el Parlamento Europeo en marzo de 2024³⁴, a la que posteriormente nos referiremos con detalle. Simplemente adelantaremos que uno de los cambios más relevante de la nueva normativa es el avance en la definición de producto defectuoso lo que se vincula en el artículo 7 a la falta de seguridad que el público en general tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional.

No cabe duda, por otro lado, de que este planteamiento ofrece una salida a la problemática planteada, sin perjuicio de que a su vez presente como nuevo reto, tampoco de fácil solución, el análisis y la precisa delimitación de los parámetros de seguridad exigibles en cada supuesto. Por nuestra parte, ante la necesidad de adoptar una postura clara, creemos que no cabe sino la apuesta clara y sin matices por la no exoneración de responsabilidad por la imprevisibilidad del acontecimiento, o el desconocimiento de los riesgos conforme al estado de la ciencia, aplicándose un régimen de responsabilidad objetiva al daño causado en esta situación³⁵.

Finalmente, en opinión de ATIENZA NAVARRO³⁶, la autonomía del sistema de inteligencia artificial no puede ser causa de exoneración para los sujetos responsables, por lo que explica esta autora que es “muy importante que se precise, cuando la responsabilidad es de carácter subjetivo, que el hecho de que el sistema actúe de manera autónoma, y adopte decisiones imprevisibles, e incluso inevitables para sus operadores, no implica, en si misma considerada, que su actuación sea diligente o que el daño se haya causado por un caso fortuito que permitiría su exoneración”. En nuestra opinión, sólo en los casos de fuerza mayor, esto es, en situaciones en las que el evento dañoso proceda de riesgos externos y, por tanto, ajenos al círculo de actividad del sistema, debemos admitir una exoneración de responsabilidad. Y del mismo modo, no existiría responsabilidad, en los supuestos de culpa exclusiva de la víctima, siempre que exista una suficiente información³⁷.

³⁴ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, (COM/2022/495 final; 2022/0302(COD)). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0495>

³⁵ De utilizarse esta causa de exoneración para los robots, sostiene DIEZ ALABART, debería establecerse al menos una excepción para los robots que interactúen con personas vulnerables (enfermos, ancianos, niños) y para los robots que tengan contacto físico con las personas. DÍAZ ALABART, S., *Robots y responsabilidad civil*, op.cit., pp. 113. Vid. ERCILLA GARCÍA, J., *Normas de Derecho Civil y Robótica*, Thomson Reuters, Pamplona, 2018, p. 75.

³⁶ ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, op.cit., p. 410.

³⁷ En esta línea de pensamiento, vid. NÚÑEZ ZORRILLA, M^a C., *Inteligencia artificial y responsabilidad civil*, op. cit., pp. 70 y ss.

Sentadas estas consideraciones previas, analizaremos el planteamiento legislativo en materia de inteligencia artificial y responsabilidad civil en el ámbito de la Unión Europea que, al menos de momento, ofrece respuestas menos ambiciosas que las apuntadas.

2.2. EL POSICIONAMIENTO INICIAL DE LA UNIÓN EUROPEA EN MATERIA DE RESPONSABILIDAD CIVIL DE LOS ROBOTS Y LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

El impacto en el orden social de la inteligencia artificial y la robótica, y su aplicación en sectores estratégicos de la economía es un fenómeno que no puede pasar desapercibido para el Derecho³⁸. Se hace, así, evidente la urgente necesidad de definir las condiciones de legitimidad jurídica de los nuevos sistemas robóticos y establecer con precisión un régimen claro de derechos y obligaciones³⁹. El rápido y continuo desarrollo de las aplicaciones y dispositivos de IA ha producido un escenario en el que el derecho precisa ofrecer soluciones a la responsabilidad por el daño causado por ellos y, en último término, por los robots⁴⁰.

De hecho, en los últimos años una de las preocupaciones constantes en la Unión Europea, además de regular su uso y los límites que necesariamente deben imponerse, ha sido la relativa al resarcimiento de los daños que pudieran ocasionarse en la utilización de estas nuevas tecnologías, asumiendo desde un primer momento que el tratamiento no podía ser el tradicionalmente empleado en la materia. Fundamentalmente, porque las características propias y específicas de las tecnologías digitales, y entre ellas, la autonomía, puede dificultar la determinación del sujeto responsable del daño y, en consecuencia, reducir las posibilidades de éxito de una reclamación en materia de responsabilidad civil⁴¹.

Es precisamente la mencionada autonomía la que plantea el principal reto del futuro, e incluso del presente. Pensamos en máquinas capaces de actuar en un determinado ámbito que puedan tomar sus “propias” decisiones,

³⁸ Sobre este tema, *vid.* GUTIÉRREZ BARRENENGOA, A.-MONJE BALMASEDA, O., “Algunas aplicaciones concretas de la robótica en ámbitos de actuación socioeconómicos. Interactuación posible y, en especial, la responsabilidad civil de los robots”, *Foro galego*, núm. 208, enero-diciembre, A Coruña, 2020, pp. 131 y ss.

³⁹ BARRIO ANDRÉS, M., “De Nuevo Sobre la Persona Robótica”, *Inteligencia Artificial*, 73, 2024, p. 66.

⁴⁰ MONTERROSO CASADO, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, *op. cit.*, p. 139.

⁴¹ GARCÍA HERRERA, V., “Panorama legislativo de la inteligencia artificial en la Unión Europea”, en LLEDÓ YAGÜE, F.; BENÍTEZ ORTUZAR, I.; *et al.*, (Dir.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, Madrid, 2021, pp. 271-272.

en razón del entorno y de las órdenes que se les den, en función de la programación con que hayan sido configuradas. Sería el caso, por ejemplo, de las prótesis robóticas, los robots para el cuidado de las personas, o los sistemas quirúrgicos o de cirugía computarizados⁴².

Sin embargo, de la complejidad y autonomía de funcionamiento de los sistemas no puede derivarse la ausencia de respuesta ante un supuesto en el que el daño efectivamente se ha producido, lo cual reduciría la confianza en los avances tecnológicos de los ciudadanos y, en la materia que nos ocupa, de los mismos profesionales sanitarios, con la consiguiente paralización del desarrollo futuro de los sistemas. Explica NAVARRO MENDIZÁBAL⁴³ que de la exigencia ética de no dañar se deduce la necesidad de resarcir el daño y en eso consiste la responsabilidad civil: establecer una norma clara de quién y en qué circunstancias tiene que responder del daño causado. Si un vehículo autónomo atropella a un viandante, si un detector inteligente de fuego no funciona y se produce un incendio o si un robot quirúrgico falla en plena operación, debe haber un responsable y una indemnización del daño causado. Lo contrario sería devastador para la confianza que podamos tener en la IA. En este contexto, la responsabilidad civil es una pieza clave porque garantiza que quien sufra un daño sea resarcido y reciba una indemnización promoviendo la innovación en sistemas IA que sean más eficientes al evitar la causación de daños.

Con este objetivo, como resultado de la labor desarrollada por el grupo de trabajo creado en 2015 por la Comisión de Asuntos Jurídicos de la Unión, el 31 de mayo de 2016, se publicó un borrador de informe con recomendaciones destinadas a la Comisión sobre las normas de Derecho civil sobre robótica⁴⁴, a fin de “asegurar que los robots estén y sigan estando al servicio de los seres humanos”⁴⁵. Se trataba de un Proyecto, aprobándose

⁴² GÓMEZ-RIESGO TABERNERO DE PAZ, J., “Los robots y la responsabilidad civil extracontractual” en BARRIO ANDRÉS, M. (Dir.), *Derecho de los robots*, La Ley-Wolters Kluwer, 2ª ed., Madrid, 2019, p. 148.

⁴³ NAVARRO MENDIZÁBAL, I., “¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos”, *op. cit.*, p. 8.

⁴⁴ Con estas Recomendaciones se pretende que la Comisión Europea realice propuestas normativas detalladas para prevenir y dar respuesta legal a las distintas cuestiones que pueda suscitar la robótica y su desarrollo futuro, dotando de un marco jurídico-normativo a la Unión Europea en su conjunto, armonizando y regulando toda esta materia con carácter supranacional, dadas las implicaciones transfronterizas que pueden surgir con la creación y comercialización de robots en los distintos Estados miembros, evitando su diferente regulación.

⁴⁵ En todo caso, sobre el fenómeno de la inteligencia artificial en el ámbito jurídico europeo desde sus primeras iniciativas, *vid.* LACRUZ MANTECÓN, M., *Robots y Personas. Una aproximación jurídica a la subjetividad cibernética*, Reus, Madrid, 2020, pp. 89 y ss. Igualmente, *vid.* ZURITA MARTÍN, I., *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, *op. cit.*, pp. 33 y ss.

el texto definitivo mediante Resolución del Parlamento Europeo de 16 de febrero de 2017⁴⁶.

Sin perjuicio de los avances posteriores, y del abandono o matización de algunos de sus postulados, se trata de un documento fundamental en la materia que nos ocupa, en la medida que sienta las bases y principios de la futura normativa europea en materia de la responsabilidad civil de los robots y los sistemas de inteligencia artificial.

En el campo de la medicina, la citada Resolución hace hincapié en la necesidad de definir los requisitos profesionales mínimos que deberá cumplir un cirujano para operar y estar autorizado a utilizar robots quirúrgicos, y considera fundamental que se respete el principio de autonomía supervisada de los robots, en virtud del cual la programación inicial de los cuidados y la elección final sobre la ejecución pertenecen en todo caso al ámbito de decisión de un cirujano humano; subraya la especial importancia que reviste la formación de los usuarios para que puedan familiarizarse con los requisitos tecnológicos en este ámbito; llama la atención acerca de la creciente tendencia al autodiagnóstico mediante el uso de robots móviles y, por consiguiente, de la necesidad de formar a los médicos para que puedan tratar los casos de autodiagnóstico; considera que la utilización de estas tecnologías no debería disminuir ni perjudicar la relación entre médico y paciente, sino proporcionar al médico una asistencia para el diagnóstico y/o tratamiento de los pacientes, con el fin de reducir el riesgo de error humano y aumentar la calidad y la esperanza de vida (Recomendación 33).

En el ámbito de la “rehabilitación e intervención en el cuerpo humano”, la Resolución de febreros 2017 pone especial énfasis, en el ilusionante futuro que implica el uso de la robótica en la medicina. Como en el caso de las “prótesis robóticas”, donde se destaca que, debe “garantizarse” el acceso continuo y sostenible al mantenimiento, la mejora y, en particular, las actuaciones de software que subsanan fallos y vulnerabilidades (Recomendación 37).

En materia de responsabilidad civil, la Resolución del Parlamento Europeo de 16 de febrero de 2017, planteó como posible solución jurídica que debía ser objeto de consideración, “crear a largo plazo una personalidad jurídica para los robots de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones

⁴⁶ Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103 (INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

autónomas inteligentes o interactúen con terceros de forma independiente” (Recomendación 59).

De este modo, la personificación de los robots autónomos pretendía dar respuesta a creciente autonomía de los robots y servir de base del sistema de responsabilidad civil que precisan estas nuevas tecnologías. Esta propuesta fue criticada sin matices en el Dictamen del Comité Económico y Social Europeo de 31 de mayo de 2017 en el que se descarta la comparación con la responsabilidad de las sociedades, y se concluye que el Comité está en contra de la introducción de cualquier tipo de personalidad jurídica para los robots o la IA, puesto que daría lugar a un posible uso indebido⁴⁷. Lo mismo sucede en la Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, que concluye que los sistemas de IA no tienen personalidad jurídica⁴⁸.

Del mismo modo, la propuesta de creación de una personalidad jurídica específica para los robots ha sido, con razón, muy criticada en la doctrina, concluyendo que “el robot no debe tener personalidad jurídica”⁴⁹, al considerarse que no es necesario complicar el sistema “para cumplir lo que el derecho de daños ya hace adecuadamente, mediante la imputación objetiva y una correcta delimitación del círculo de responsables”⁵⁰, y que la respuesta jurídica a los daños causados por los robots, “pasa por recurrir a soluciones consolidadas, como la establecer una responsabilidad objetiva y repartir la carga de la indemnización entre grupos sociales concretos, o la de imputar la responsabilidad al ser humano que esté relacionado con el robot causante de los daños”⁵¹.

Finalmente, según la mencionada Resolución de 2017, los daños y perjuicios causados por robots se consideran una cuestión fundamental que debe

⁴⁷ Dictamen del Comité Económico y Social Europeo (CESE) sobre la “Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad” (2017/C 288/01). (<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016IE5369&from=BG>).

⁴⁸ Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)).

https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html

⁴⁹ GIL MEMBRADO, C., “Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el derecho”, en GIL MEMBRADO, C. (Dir. y Coord.), *Bioderecho y retos. M-Health, Genética, IA, Robótica y criogenización*, Dykinson, Madrid, 2022, p. 364.

⁵⁰ RUBI PUIG, A., “Retos de la inteligencia artificial y adaptabilidad del derecho de daños”, *op. cit.*, p. 68.

⁵¹ LACRUZ MANTECÓN, M., *Robots y Personas. Una aproximación jurídica a la subjetividad cibernética*, *op. cit.*, p. 179. Igualmente, *vid.* ZURITA MARTÍN, I., *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, *op. cit.*, p. 46; ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, *op. cit.*, p. 410.

analizarse a nivel de la UE para garantizar el mismo grado de eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica de los ciudadanos, los consumidores y las empresas (Recomendación 49), y considera que para elaborar la futura legislación debe evaluarse si aplicar el enfoque de la responsabilidad objetiva o el de la gestión de riesgos (Recomendación 53). A tal efecto, manifiesta que la responsabilidad objetiva “únicamente exige probar que se ha producido un daño o perjuicio y el establecimiento de un nexo causal entre el funcionamiento perjudicial del robot y los daños o perjuicios causados a la persona que los haya sufrido” (Recomendación 54) y “el enfoque de gestión de riesgos no se centra en la persona “que actuó de manera negligente” como personalmente responsable, sino en la persona que es capaz, en determinadas circunstancias, de minimizar los riesgos y gestionar el impacto negativo” (Recomendación 55)⁵².

Por todo ello, en la Resolución se solicita la presentación, sobre la base del artículo 114 del TFUE, de una propuesta de instrumentos legislativos sobre los aspectos jurídicos relacionados con el desarrollo y el uso de la robótica y la inteligencia artificial previsibles en los próximos diez o quince años, junto con instrumentos no legislativos -por ejemplo, directrices y códigos de conducta-.

En la línea anunciada, en un primer intento de abordar la cuestión nos encontramos con la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, a la que acompañaba una propuesta de Reglamento para regular la responsabilidad civil por el funcionamiento de estos sistemas⁵³.

Con ella, se seguía el camino iniciado por el Informe de la Comisión Europea de 19 de febrero de 2020, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, hacer algunos ajustes en los regímenes de responsabilidad civil nacionales a través de iniciativas adecuadas de la UE, sobre la base de un enfoque específico basado en el riesgo, es decir, teniendo en cuenta que las distintas aplicaciones de IA presentan riesgos diferentes⁵⁴.

Concretamente, en el anexo a la Resolución de 20 de octubre de 2020, se destacaban una serie de principios que debían servir de orientación en la

⁵² MONTERROSO CASADO, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, *op. cit.*, pp. 127-128.

⁵³ Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html

⁵⁴ Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social europeo. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020 (COM (2020) 64 final).

materia, partiendo, como primer principio, de que un mercado único digital genuino requiere una armonización completa mediante un Reglamento. Así, considerando que las normas de responsabilidad civil para la IA deben tratar de lograr un equilibrio entre la protección del público, por una parte, y los incentivos empresariales para invertir en innovación, especialmente en sistemas de IA, por otra, se establece como objetivo, en lugar de sustituir los regímenes de responsabilidad civil existentes, que funcionan correctamente, deben realizar algunos ajustes necesarios mediante la introducción de ideas nuevas y orientadas al futuro.

Para ello, se afirmaba que la futura propuesta de Reglamento y la Directiva sobre responsabilidad por los daños causados por productos defectuosos constituyen los dos pilares de un marco común de responsabilidad civil para los sistemas de IA y requieren una estrecha coordinación y concertación entre todos los agentes políticos, a nivel nacional y de la Unión, ya que, como también se destaca en el anexo a la Resolución, los ciudadanos deben tener derecho al mismo nivel de protección y de derechos, independientemente de si el daño es causado por un sistema de IA o no, o de si tiene lugar física o virtualmente, de tal forma que aumente su confianza en la nueva tecnología⁵⁵.

En este sentido, en la propuesta de Reglamento que acompañaba a la Resolución de 20 de octubre de 2020, se establecía una serie de normas en relación con las demandas de responsabilidad civil de las personas físicas y jurí-

⁵⁵ En estas novedosas reglas especiales para la IA, formuladas como una propuesta de Reglamento, como explica GONZÁLEZ BELUCHE, se distinguían dos potenciales responsables: el operador inicial (“back-end operator”), que era, según el art.3 e), aquel sujeto encargado de definir las características de la tecnología, de proveer datos y de prestar un servicio de apoyo final esencial para la operatividad del sistema (v.gr. el fabricante de un robot para la domótica); y el operador final (“front-end operator”), que se identificaba, de acuerdo con el art. 3 f), con aquella persona que ejercía cierto control sobre el riesgo asociado al funcionamiento del sistema de inteligencia artificial, beneficiándose de él (v.gr. el usuario del robot). Diferenciados los operadores, la responsabilidad del operador inicial (“back-end operator”) era remitida a la Directiva de productos defectuosos -la cual, precisamente por ello, debía ser modificada- y cuando el sistema de IA causara daños, se preveía, fundamentalmente respecto del operador final, un régimen general de responsabilidad por culpa y otro, de responsabilidad objetiva, para casos excepcionales de sistemas del alto riesgo -que se prevenía que deberían ser recogidos en un anexo al Reglamento (Cdo.16)-. GONZÁLEZ BELUCHE, P., “La adaptación de la Directiva 85/374/CEE, de 25 de julio, en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución industrial”, *Cuadernos de Derecho Transnacional*, vol. 15, n° 2, 2023, p. 452.

En todo caso, conforme al artículo 11, en caso de que haya más de un operador de un sistema de IA, estos serán responsables solidarios. Si un operador final es también el productor del sistema de IA, el presente Reglamento prevalecerá sobre la Directiva sobre responsabilidad por los daños causados por productos defectuosos. Si el operador inicial también tiene la condición de productor en el sentido del artículo 3 de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, deberá aplicársele dicha Directiva. Si solo hay un operador y dicho operador es también el productor del sistema de IA, el presente Reglamento prevalecerá sobre la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

dicas contra los operadores de sistemas de IA. De este modo, como instrumento normativo se proponía un Reglamento que se aplicaría en el territorio de la Unión a aquellos casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable, siendo nulo todo acuerdo que eluda o limite los derechos y obligaciones establecidos en el Reglamento. Todo ello, además, sin perjuicio de cualquier otra demanda en materia de responsabilidad civil derivada de las relaciones contractuales, así como de la normativa sobre responsabilidad por los daños causados por productos defectuosos, la protección de los consumidores, la lucha contra la discriminación y la protección laboral y del medio ambiente, que se pueda presentar contra el operador de conformidad con el Derecho de la Unión o nacional.

La propuesta se completaba, a nuestro juicio con acierto, con un sistema de responsabilidad objetiva de los sistemas de IA de alto riesgo⁵⁶, que serían objeto de enumeración en el anexo del Reglamento, sin perjuicio de que se preveía que pudieran ser modificados constantemente por la Comisión mediante actos delegados.

En estos casos, los operadores de un sistema de IA de alto riesgo no podían eludir su responsabilidad civil alegando que actuaron con la diligencia debida o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA, aunque se indicaba en el mismo artículo 4 de la propuesta de Reglamento, que los operadores no serán responsables si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. Como necesario complemento, se establecían diferentes seguros de responsabilidad civil tanto para el operador inicial como final del sistema de IA, regulando el artículo 5 el importe de las indemnizaciones⁵⁷.

⁵⁶ En esta línea, pronosticaba con acierto EBERS, que ante este trasfondo podría considerarse si de *lege ferenda* - eventualmente incluso a nivel europeo - no debería ser tipificado un nuevo supuesto de hecho de la responsabilidad por riesgo para el operador. El atractivo de una tal solución es obvio, explicaba con rigor este autor. Tratándose de la responsabilidad por riesgos imprevisibles, que derivan de una tecnología socialmente deseada, pero peligrosa, la responsabilidad por riesgo presenta los mejores instrumentos en comparación con la responsabilidad por culpa. EBERS, M., “La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de responsabilidad civil?”, *InDret. Revista para el Análisis del Derecho*, núm. 3, Barcelona, 2016, p. 15.

⁵⁷ Ciertamente, como excesiva limitación, se planteaba que cuando la indemnización combinada que deba abonarse a varias personas que sufran daños o perjuicios causados por el mismo funcionamiento de un mismo sistema de IA de alto riesgo supere los importes totales máximos previstos, los importes que deban abonarse a cada persona se reducirán proporcionalmente de forma que la indemnización combinada no supere los importes máximos establecidos. En cambio, nos encontramos ante amplios plazos de prescripción en el artículo 7, de 30 años en los daños físicos, y de 10 o 30 años en casos de daños materiales y morales.

Por otro lado, el operador de un sistema de IA, que no constituya un sistema de alto riesgo, estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA. El operador no podrá eludir su responsabilidad alegando que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA, pero, al igual que en el supuesto de sistemas de alto riesgo, no será responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor.

Con independencia de que el sistema de IA sea de alto riesgo u otro sistema, si el daño o perjuicio es causado por una actividad física o virtual, un dispositivo o un proceso gobernados por un sistema de IA o por la actuación de una persona afectada o de una persona de la que la persona afectada sea responsable, el alcance de la responsabilidad civil del operador con arreglo al Reglamento se reducirá en consecuencia, estableciéndose igualmente en el artículo 10 de la Propuesta de Reglamento que el operador no será responsable si la persona afectada o la persona de la que esta es responsable es la única a la que se le puede achacar el daño o perjuicio causado, lo cual nos conducirá necesariamente a la exigencia de que la información que ha recibido la persona debe ser sea todo momento suficiente y completa.

Sin embargo, este camino fue modificado con la aprobación de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, de 28 de septiembre de 2022 aplicable a demandas civiles extracontractuales, cuando dichas demandas se presenten sobre la base de la existencia de una culpa, que hasta el momento no ha contado con avances importantes en su tramitación⁵⁸, y la Propuesta de Directiva del Parlamento europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, también de 28 de septiembre de 2022, que fue objeto de aprobación por el Parlamento Europeo el 12 de marzo de 2024⁵⁹.

Se abandona, por tanto, la idea de regular la responsabilidad de daños causados por sistemas de IA a través de un Reglamento, optando por actuar también en esa materia a través de una Directiva por su mayor flexibilidad, dada la existencia de importantes diferencias entre los distintos ordenamientos de la Unión Europea.

⁵⁸ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), (COM/2022/496 final; 2022/0303(COD)). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>

⁵⁹ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, (COM/2022/495 final; 2022/0302(COD)). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0495>

La publicación de las dos propuestas de Directiva, explica acertadamente GONZÁLEZ BELUCHE⁶⁰, apunta a que podrá exigirse responsabilidad a los productores, incluyendo a los de sistemas de IA y productos digitales, con base en la Directiva sobre Responsabilidad civil por productos defectuosos, una vez ésta sea modificada para solucionar los problemas de adaptación a las nuevas tecnologías. Mientras que, cuando se trate de reclamar la responsabilidad de otros sujetos (por ejemplo, del usuario del sistema de IA, *vid.* Cdo.15), deberán invocarse los sistemas de los Estados miembros de responsabilidad por culpa, que deberán adaptarse a lo previsto en la Propuesta de Directiva de IA para introducir las medidas armonizadoras. Medidas que, una vez incorporadas, homogeneizarán los sistemas nacionales, aumentando la seguridad jurídica (Cdo. 9 Propuesta de Directiva de IA) a los regímenes nacionales de responsabilidad por culpa, que deberán adecuar y armonizar sus normas -en materia de la carga probatoria- para resolver aquellas reclamaciones en las que haya sistemas de IA implicados.

2.3. LAS PROPUESTAS DE REGULACIÓN DE LA UE: LA DIRECTIVA SOBRE RESPONSABILIDAD POR DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS Y LA DIRECTIVA RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL A LA INTELIGENCIA ARTIFICIAL

En la Unión Europea, la normativa de responsabilidad civil ha descansado en la aplicación paralela de los regímenes nacionales no armonizados y la Directiva 85/374/CEE sobre responsabilidad por los daños causados por productos defectuosos⁶¹. Precisamente, esta Directiva será derogada por la propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022⁶², que ha sido objeto de aprobación por el Parlamento Europeo en marzo de 2024⁶³.

⁶⁰ GONZÁLEZ BELUCHE, P., “La adaptación de la Directiva 85/374/CEE, de 25 de julio, en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución industrial”, *op.cit.*, p. 454.

⁶¹ Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, cuya trasposición en España se llevó a efecto a través de la Ley 22/1994, de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos, hoy refundida en el TRLDCU 1/2007.

⁶² Propuesta de Directiva del Parlamento europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. COM (2022) 495 final, 2022/0302 (COD). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0495>; El texto final de la Directiva, que se contiene en la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM(2022)0495 - C9-0322/2022 - 2022/0302(COD)) está disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.html

⁶³ Conforme al artículo 21 de la propuesta, la Directiva 85/374/CEE quedará derogada veinticuatro meses después de la fecha de entrada en vigor de la presente Directiva. No obstante,

Con ello, comienza un proceso de adaptación legislativa a la nueva realidad a la que conduce la implantación y utilización generalizada de la inteligencia artificial en nuestra vida ordinaria. Se trata, en todo caso, de una modificación sustancial del régimen actual que, sin embargo, debemos lamentar que sólo sea aplicable a los productos introducidos en el mercado o puestos en servicio una vez transcurridos veinticuatro meses de su entrada en vigor (art. 2.1), lo que supone que la reforma se aplicará únicamente a los productos puestos en el mercado desde el momento en que los Estados miembros deban haber cumplido con su obligación de transposición, de acuerdo al artículo 22 de la Directiva, ya que ambas fechas coinciden.

No podemos valorar positivamente la ampliación del plazo inicialmente previsto para la transposición y entrada en vigor, que se situaba en doce meses en el primer texto, ya que supone retrasar la aplicación de una serie de soluciones legales que nadie duda que son necesarias ahora, al margen de que tampoco consideramos adecuado actuar a veinticuatro meses vista en una materia en la que los avances son especialmente rápidos y el futuro de difícil pronóstico. A ello se suma que, aunque la Directiva 85/374/CEE quedará derogada veinticuatro meses después de la entrada en vigor de la nueva normativa, su régimen de responsabilidad seguirá aplicándose a aquellos productos introducidos en el mercado con anterioridad.

En lo que a nosotros ocupa, en el nuevo texto se acaba con las dudas de si un programa informático es o no un producto, ya que se afirma claramente que lo es, al definir “producto” en el artículo 4 de la Directiva, como cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; también la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos⁶⁴.

En esta línea, se explica con detalle en el considerando 13 que los productos en la era digital pueden ser tangibles o intangibles, y que los programas informáticos, como los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. De este modo, se añade en el considerando citado que los programas informáticos pueden introducirse en el mercado como productos autónomos o, posteriormente, pueden integrarse en otros produc-

seguirá aplicándose a los productos introducidos en el mercado o puestos en servicio antes de esa fecha.

⁶⁴ De este modo, explica NAVARRO MENDIZÁBAL, que se busca incluir en la responsabilidad civil de productos defectuosos a aquellos productos que tengan sistemas de IA, lo cual entiendo correcto porque la IA no existe de forma aislada, sino que opera en un determinado producto. NAVARRO MENDIZÁBAL, I., “¿Quién paga los daños ...”, *op. cit.*, p. 12.

tos como componentes, y pueden causar daños al ejecutarse, indicando también que en aras de la seguridad jurídica, debe aclararse que los programas informáticos son un producto a efectos de la aplicación de la responsabilidad objetiva, independientemente de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo, se accede a él a través de una red de comunicaciones o tecnologías en la nube o se suministra a través de un modelo de programa informático como servicio⁶⁵.

Para terminar, a los efectos de despejar posibles dudas, se destaca expresamente en el considerando 13 que un desarrollador o productor de programas informáticos, incluidos los proveedores de sistemas de IA en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo⁶⁶, debe ser tratado como un fabricante.

En todo caso, conforme al artículo 2.2 la Directiva no es de aplicación a los programas informáticos libres y de código abierto que se desarrollen o suministren fuera del transcurso de una actividad comercial, lo cual consideramos adecuado no sólo debido a que en muchas ocasiones no será posible identificar al autor de los programas, sino en atención a que su puesta en el mercado no obedece a intereses comerciales.

Por otro lado, uno de los cambios más relevante de la nueva normativa es el avance en la definición de producto defectuoso⁶⁷, lo que se vincula a la falta de seguridad que el público en general tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional (artículo 7), estableciendo en el artículo 9.2 una presunción del carácter defectuoso, cuando el demandado no haya exhibido las pruebas pertinentes de conformidad con el artículo 10, apartado 1; el demandante demuestre que el producto no cumple los requisitos obligatorios de seguridad del producto establecidos en el Derecho de la Unión o en la legislación nacional que tienen por objeto proteger contra el riesgo del daño sufrido por la persona perjudicada; o el

⁶⁵ Sin embargo, matiza el considerando 13, que la información no debe considerarse un producto, por lo que las normas sobre responsabilidad por productos defectuosos no deben aplicarse al contenido de los archivos digitales, como los archivos multimedia o los libros electrónicos o el mero código fuente de los programas informáticos.

⁶⁶ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de inteligencia artificial) (DO L, 2024/1689 de 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).

⁶⁷ RAMÓN FERNÁNDEZ, F., “El robot como producto defectuoso y responsabilidad civil”, *Derecho Digital e Innovación*, n.º 14, Sección Doctrina, Cuarto trimestre de 2022, (LA LEY 10941/2022), pp. 6 y ss.

demandante demuestra que el daño fue causado por un mal funcionamiento evidente del producto durante un uso razonablemente previsible o en circunstancias normales.

Del mismo modo, se establece una presunción del nexo causal entre el carácter defectuoso y el daño, conforme al artículo 10.3, cuando se haya comprobado que el producto es defectuoso y el daño causado sea de un tipo compatible normalmente con el defecto en cuestión, a lo que se añade en el apartado 4 del artículo 10 que el órgano jurisdiccional nacional presumirá el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambas cosas, cuando, a pesar de la exhibición de pruebas de conformidad con el artículo 9 y teniendo en cuenta todas las circunstancias pertinentes del caso, el demandante se enfrente a dificultades excesivas, en particular debido a la complejidad técnica o científica para demostrar el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambas cosas; y el demandante demuestre que es probable que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso y el daño, o ambos⁶⁸.

Resulta evidente la preocupación del legislador en evitar que la complejidad técnica de los productos, lo cual es evidente en los que incorporan sistemas de inteligencia artificial, impidan o dificulten el resarcimiento de los daños sufridos por personas físicas caudados por productos defectuosos.

En esta línea, se destaca en la nueva Directiva (considerando 48), que los órganos jurisdiccionales nacionales deben presumir el carácter defectuoso de un producto o el nexo causal entre el daño y el defecto, o ambos, cuando, a pesar de la revelación de información por parte del demandado, resulte excesivamente difícil para el demandante, en especial debido a la complejidad técnica o científica del caso, demostrar su carácter defectuoso o el nexo causal, o ambas cosas. Deben hacerlo teniendo en cuenta todas las circunstancias del asunto. En tales casos, se añade en la Directiva que imponer nivel de prueba habitual exigido por el Derecho nacional, que a menudo requiere un alto grado de probabilidad, socavaría la efectividad del derecho a indemnización. Por lo tanto, dado que los fabricantes tienen conocimientos especializados y están mejor informados que la persona perjudicada, y a fin de mantener un reparto equitativo del riesgo, al tiempo que se evita una inversión de la carga de la prueba, se concluye que debe exigirse al demandante que demuestre, cuando sus dificultades

⁶⁸ Con carácter general, sobre las presunciones en esta materia, *vid.* EVANGELIO LLORCA, R., “Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE”, en ÁLVAREZ LATA, N. (Coord.), *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, Pamplona, 2024, pp. 549 y ss.

se refieran a la prueba del carácter defectuoso del producto, únicamente que es probable que el producto fuera defectuoso, o, cuando las dificultades del demandante se refieran a la prueba del nexo causal, únicamente que el carácter defectuoso del producto es una causa probable del daño.

Por último, la complejidad técnica o científica, según el mencionado considerando 48, debe ser determinada por los órganos jurisdiccionales nacionales caso por caso, teniendo en cuenta diversos factores. Estos factores deben incluir la naturaleza compleja del producto, como un producto sanitario innovador; la naturaleza compleja de la tecnología utilizada, como el aprendizaje automático; la naturaleza compleja de la información y los datos que debe analizar el demandante; y la naturaleza compleja del nexo causal, como la relación entre un producto farmacéutico o alimenticio y la aparición de una enfermedad, o una relación que, para ser probada, requeriría que el demandante explicara el funcionamiento interno de un sistema de IA. La evaluación de las dificultades excesivas también debe ser realizada por los órganos jurisdiccionales nacionales, caso por caso. Si bien el demandante debe aportar argumentos para demostrar la existencia de dificultades excesivas, no debe exigirse la prueba de tales dificultades.

Así, se explica en el considerando 48 que, por ejemplo, en una demanda relativa a un sistema de IA, para que el órgano jurisdiccional decida que existen dificultades excesivas, no debe exigirse al demandante que explique las características específicas del sistema de IA ni cómo estas características dificultan la determinación del nexo causal. El demandado debe tener la posibilidad de impugnar todos los elementos de la demanda, incluida la existencia de dificultades excesivas.

En definitiva, el avance de la Directiva es significativo en relación con las menores exigencias en materia de la carga de la prueba en las situaciones en las que un sistema de IA está implicado⁶⁹, lo cual debe valorarse positivamente. Se presta adecuada atención a la creciente complejidad de los productos y la nueva realidad a la que nos enfrentamos como consumidores. Con esta propuesta, se solucionan de una vez por todas las dudas habituales sobre quién responderá si un coche autónomo causa daños o si el robot quirúrgico Da Vinci falla o qué ocurre con una app que usa un algoritmo cuyos resultados causan daños al usuario⁷⁰, enumerando con detalle el artículo 8 de la Directiva quienes son los operadores económicos responsables de los productos defectuosos, entre los que se incluye, según indica el considerando 13,

⁶⁹ Sobre esta materia, *vid.* JORQUI AZOFRA, M., *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023, pp. 1 y ss.

⁷⁰ NAVARRO MENDIZÁBAL, I., “¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos”, *op. cit.*, p. 13.

el desarrollador del software. No obstante, es preciso esperar a la trasposición de la Directiva que efectúen los Estados miembros para determinar el alcance real de la protección que dispensará a los consumidores.

Sin embargo, no ha sido esta Directiva la única iniciativa de la Unión Europea en el tema. Nos referimos a la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, de 28 de septiembre de 2022 aplicable a demandas civiles extracontractuales, cuando dichas demandas se presenten sobre la base de la existencia de una culpa, sin grandes avances de momento en su tramitación⁷¹, y que constituye la primera propuesta de armonización específica de las legislaciones nacionales sobre responsabilidad civil en materia de IA, con el objetivo de modernizarlas introduciendo unas normas específicas para los daños causados por los sistemas de IA y facilitando que las víctimas obtengan una indemnización.

La propuesta de Directiva, como anuncia en su Exposición de motivos se basa en un enfoque por fases. La primera fase se limita a las medidas relativas a la carga de la prueba para hacer frente a los problemas propios de la IA detectados. Se basa en las condiciones sustantivas de responsabilidad civil que existen actualmente en las normas nacionales, como la causalidad o la culpa, pero se centra en medidas específicas relacionadas con la prueba, garantizando que las víctimas tengan el mismo nivel de protección que en los casos en los que no medien sistemas de IA. La segunda fase incluida en la propuesta garantiza que, a la hora de evaluar el efecto de la primera fase en términos de protección de las víctimas y adopción de la IA, se tengan en cuenta los futuros cambios tecnológicos, normativos y jurisprudenciales a la hora de reevaluar la necesidad de armonizar otros elementos de las demandas de indemnización u otros instrumentos relacionados con las demandas de responsabilidad civil, incluido en aquellas situaciones en que la responsabilidad objetiva sería más adecuada, según lo solicitado por el Parlamento Europeo.

En todo caso, es necesario destacar que la propuesta de Directiva, que apuesta por mantener inicialmente un criterio de responsabilidad subjetiva en la materia, no contiene una regulación completa del derecho de daños⁷², sino que se aplicará junto a las distintas legislaciones nacionales funcionando como un complemento de ellas, facilitando la prueba del demandante y esta-

⁷¹ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), (COM/2022/496 final; 2022/0303(COD)). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>.

⁷² ORTÍZ FERNÁNDEZ, M., “La adaptación del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad”, *Revista de Internet, Derecho y Política*, n° 40, 2024, p. 5.

bleciendo una serie de presunciones. Los tribunales de cada Estado aplicarán su legislación interna, teniendo en cuenta las reglas contenidas en la propuesta, que deberán ser objeto de transposición a los dos años de su entrada en vigor (artículo 8).

Así, en la propuesta se establecen normas uniformes sobre el acceso a la información, estableciendo en el artículo 3 la obligatoriedad de que los Estados miembros garanticen que los órganos jurisdiccionales puedan ordenar la exhibición de pruebas, sin perjuicio de las limitaciones y del respeto al principio de proporcionalidad que también se establece. De hecho, como regla a general se llega a concluir en el apartado 5 del precepto una presunción de culpabilidad cuando un demandado incumpla la orden de un órgano jurisdiccional nacional en una demanda por daños y perjuicios de exhibir o conservar las pruebas que obran en su poder, sin perjuicio de las excepciones que se establecen.

En el artículo 4 ciertamente se establece una presunción general del nexo causal y el daño, en diversos casos, pero de nuevo nos encontramos con importantes excepciones que ponen de manifiesto la excesiva prudencia con la que se actúa en la materia. En el caso de las demandas por daños y perjuicios relacionadas con sistemas de IA de alto riesgo, los órganos jurisdiccionales nacionales no aplicarán la presunción cuando el demandado demuestre que el demandante puede acceder razonablemente a pruebas y conocimientos especializados suficientes para demostrar el nexo causal (apartado 4). En el caso de las demandas por daños y perjuicios relacionadas con sistemas de IA que no sean de alto riesgo, la presunción establecida solo se aplicará cuando el órgano jurisdiccional nacional considere excesivamente difícil para el demandante demostrar el nexo causal (apartado 5). En el caso de las demandas por daños y perjuicios contra un demandado que haya utilizado el sistema de IA en el transcurso de una actividad personal de carácter no profesional, la presunción establecida solo se aplicará cuando el demandado haya interferido sustancialmente en las condiciones de funcionamiento del sistema de IA o cuando el demandado tuviese la obligación y estuviese en condiciones de determinar las condiciones de funcionamiento del sistema de IA y no lo haya hecho (apartado 6).

En definitiva, en la propuesta de Directiva se reduce notablemente la carga de la prueba en relación con los daños provocados por los sistemas de IA, sin llegar a plantear, para no perjudicar a las empresas, del sector una inversión de la carga de la prueba, como sería deseable. Es éste, precisamente, el punto más discutible del texto, especialmente en lo que se refiere a la aplicación de esos principios en el ámbito sanitario.

BIBLIOGRAFÍA UTILIZADA

- ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022.
- BARRIO ANDRÉS, M., “Los principios generales de los Derechos de los Robots” en BARRIO ANDRÉS, M. (Dir.), *Derecho de los robots*, La Ley-Wolters Kluwer, 2ª ed., Madrid, 2019.
- BARRIO ANDRÉS, M., “De Nuevo Sobre la Persona Robótica”, *Inteligencia Artificial*, 73, 2024.
- BADILLO ARIAS, J.A., “Responsabilidad civil y aseguramiento obligatorio de los robots”, en MONTERROSO CASADO, E., (Dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Tirant lo blanch, Valencia, 2019.
- DÍAZ ALABART, S., *Robots y responsabilidad civil*, Editorial Reus, Madrid, 2018.
- EBERS, M., “La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de responsabilidad civil?”, en *InDret. Revista para el Análisis del Derecho*, núm. 3, Barcelona, 2016.
- ERCILLA GARCÍA, J., *Normas de Derecho Civil y Robótica*, Thomson Reuters, Pamplona, 2018.
- EVANGELIO LLORCA, R., “Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE”, en ÁLVAREZ LATA, N. (Coord.), *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, Pamplona, 2024.
- GARCÍA HERRERA, V., “Panorama legislativo de la inteligencia artificial en la Unión Europea”, en LLEDÓ YAGÜE, F.; BENÍTEZ ORTÚZAR, I.; et al., (Dir.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, Madrid, 2021.
- GIL MEMBRADO, C., “Una nueva era: hacia el robot sanitario “autónomo” y su encaje en el derecho”, en GIL MEMBRADO, C. (Dir. y Coord.), *Bioderecho y retos. M-Health, Genética, IA, Robótica y criogenización*, Dykinson, Madrid, 2022.
- GIL MEMBRADO, C., *Riesgos del uso de algoritmos en el diagnóstico y en la investigación biomédica*, Editorial Reus, Madrid, 2023.
- GÓMEZ-RIESGO TABERNERO DE PAZ, J., “Los robots y la responsabilidad civil extracontractual” en BARRIO ANDRÉS, M. (Dir.), *Derecho de los robots*, La Ley-Wolters Kluwer, 2ª ed., Madrid, 2019.
- GONZÁLEZ BELUCHE, P., “La adaptación de la Directiva 85/374/CEE, de 25 de julio, en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución industrial”, *Cuadernos de Derecho Transnacional*, vol. 15, nº 2, 2023.
- GUTIÉRREZ BARRENENGOA, A.- MONJE BALMASEDA, O., “Algunas aplicaciones concretas de la robótica en ámbitos de actuación socioeconómicos. Interactuación posible y, en especial, la responsabilidad civil de los robots”, *Foro galego*, núm. 208, enero-diciembre, A Coruña, 2020.

- JORQUI AZOFRA, M., *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, Dykinson, Madrid, 2023.
- LACRUZ MANTECÓN, M., *Robots y Personas. Una aproximación jurídica a la subjetividad cibernética*, Reus, Madrid, 2020.
- LUQUIN BERGARECHE, R., “Medicina personalizada y uso secundario de datos de salud para fines de investigación: algunas cuestiones”, *Cuadernos de Derecho Privado*, 8, 2024, pp. 69-115.
- MARTÍNEZ QUIRANTE, R.-RODRIGUEZ ÁLVAREZ, J., *Inteligencia artificial y armas letales autónomas. Un nuevo reto para Naciones Unidas*, TREA, Asturias, 2018.
- MONJE BALMASEDA, O., “Responsabilidad civil, robótica e inteligencia artificial”, en LLEDÓ YAGÜE, F.; BENÍTEZ ORTÚZAR, I.; et al., (Dir.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, Madrid, 2021.
- MONJE BALMASEDA, O., “Robótica y responsabilidad civil en el ámbito sanitario”, en GIL MEMBRADO, C. (Dir. y Coord.), *Bioderecho y retos. M-Health, Genética, IA, Robótica y criogenización*, Dykinson, Madrid, 2022.
- MONJE BALMASEDA, O., “Responsabilidad civil en el ámbito sanitario por daños causados por robots”, en MARTÍNEZ VELENCOSO, L.-PLAZA PENEDÉS J., *Retos normativos del mercado digital único europeo*, Tirant lo Blanch, Valencia, 2022.
- MONTERROSO CASADO, E., “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, en MONTERROSO CASADO, E. (Dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramientos*, Tirant lo Blanch, Valencia, 2019.
- NAVARRO MENDIZÁBAL, I., “¿Quién paga los daños que causa la IA? De la ética a la responsabilidad por productos defectuosos”, *Revista Iberoamericana de Bioética*, nº 25, 2024.
- NÚÑEZ ZORRILLA, M.C. *Inteligencia artificial y responsabilidad civil*, REUS, Madrid, 2018.
- ORTÍZ FERNÁNDEZ, M., “La adaptación del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad”, *Revista de Internet, Derecho y Política*, nº 40, 2024.
- PALMERINI, E., “Robótica y Derecho, sugerencias, confluencias, evoluciones en el marco de una investigación europea” en *Revista de Derecho privado*, nº 32, 2017.
- RAMÓN FERNÁNDEZ, F., “El robot como producto defectuoso y responsabilidad civil”, *Derecho Digital e Innovación*, nº 14, Sección Doctrina, Cuarto trimestre de 2022, (LA LEY 10941/2022).
- RUBI PUIG, A., “Retos de la inteligencia artificial y adaptabilidad del derecho de daños”, en CERDILLO I MARTÍNEZ, A.-PEGUERA POCH, M. (Coord.), *Retos jurídicos de la inteligencia artificial*, Thomson Reuters Aranzadi, Pamplona, 2020.
- ZURITA MARTÍN, I., *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Editorial Reus, Madrid, 2020.

La responsabilidad civil derivada de los accidentes de circulación ocasionados con vehículos autónomos

ESTHER MONTERROSO CASADO

esther.monterroso@udima.es

*Profesora Titular de Derecho Civil
Universidad a Distancia de Madrid*

Sumario: I. INTRODUCCIÓN. 2 EVOLUCIÓN Y REGULACIÓN DE LA RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL POR DAÑOS EN LA CIRCULACIÓN DE VEHÍCULOS A MOTOR. 2.1. Evolución legal de la responsabilidad derivada de los accidentes de circulación. 2.2. Regulación actual y perspectivas de futuro de la responsabilidad derivada de los accidentes de circulación. 3. VEHÍCULOS AUTÓNOMOS Y CONDUCCIÓN AUTOMATIZADA. 3.1. El vehículo autónomo. 3.2. Los niveles de autonomía. 3.3. Autonomía real en la oferta de conducción automatizada. 4. REGULACIÓN DE LA CONDUCCIÓN AUTOMATIZADA. 4.1. Marco jurídico europeo de vehículos automatizados y totalmente automatizados. 4.2. Marco jurídico nacional de conducción automatizada. 4.2.1. Bases del marco regulatorio: Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. 4.2.2 Proyecto legislativo en materia de conducción automatizada: modificaciones del Reglamento General de Circulación y del Reglamento General de Vehículos. 5. REGULACIÓN DE LOS SISTEMAS DE ALTO RIESGO EN LA INTELIGENCIA ARTIFICIAL. 5.1. Reglamento europeo por el que se establecen normas armonizadas en materia de inteligencia artificial. 5.2. Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos. 5.3. Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial. 6. HACIA UN NUEVO CRITERIO DE RESARCIMIENTO DE DAÑOS DERIVADO DE LA AUSENCIA DEL CONDUCTOR DEL VEHÍCULO. 6.1. Responsabilidad del fabricante del vehículo. 6.2. Responsabilidad del operador o del propietario del vehículo. 6.3. Resarcimiento del daño por la aseguradora del vehículo, tomando como referencia la LRCSCVM. 6.4. Resarcimiento del daño por la aseguradora del vehículo, sin imputación de la responsabilidad. 7. CONCLUSIONES. 8. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

Según datos de la DGT, en la actualidad, más del 90 % de los accidentes de tráfico se deben, en alguna medida, a descuidos humanos, previendo que el desplazamiento de vehículos autónomos, que incorpora sistemas para hacer la conducción, y la circulación en general, más segura, posibilitará la reducción del factor error humano, lo que implicará una disminución del número de víctimas en las carreteras¹. De hecho, uno de los grandes objetivos que pretende la Estrategia de Seguridad Vial 2030 es reducir el número de personas fallecidas y heridas graves a la mitad².

La conducción autónoma comprende un elenco de asistentes a la conducción, los llamados ADAS (por sus siglas en inglés *Advanced Driver Assistance Systems*) o Sistemas Avanzados de Asistencia al Conductor. Con la implantación de estos dispositivos, se va a producir un cambio de paradigma en el sistema de conducción, en donde el nivel de conducción autónoma de los vehículos va a depender de la capacidad que tengan estos asistentes para pilotar el vehículo sin la intervención humana.

La conducción de los vehículos autónomos implica un cambio en el rol de las personas al volante del vehículo debido a que en los niveles más avanzados de conducción autónoma el conductor llega a convertirse en un mero usuario del vehículo, lo que plantea si ello ocasiona que deba modificarse el sistema de imputación de los daños causados en los accidentes de circulación. En esta tesitura, cuando los vehículos autónomos prescindan de la figura del conductor, habrá que determinar cómo se llevará a cabo el resarcimiento de los daños causados a las víctimas y perjudicados, teniendo en cuenta, además, que en las primeras fases de implantación continuarán conviviendo en las carreteras ambas clases de vehículos, lo que sin duda supone un mayor reto jurídico a la hora de analizar la responsabilidad derivada de los daños causados en accidentes de circulación.

El objetivo de este trabajo es identificar, por un lado, el régimen de responsabilidad por accidentes de circulación cuando el conductor tenga el control sobre el mismo, y el sistema de responsabilidad cuando nos encontremos con vehículos dotados de inteligencia artificial. En este contexto, nos encon-

¹ DGT (2024) *Vehículos de conducción automatizada*, 21 marzo 2024. <https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/vehiculos-de-conduccion-automatizada/> Los vehículos autónomos contribuirán de forma importante al objetivo de la UE de cero víctimas mortales en carretera para 2050; y junto con la electrificación de vehículos o el transporte compartido permitirán optimizar la movilidad, reducir la congestión del tráfico, disminuir los costes del transporte y reducir significativamente las emisiones de CO₂.

² DGT (2024). Vehículos seguros y conectados. *Estrategia de Seguridad Vial 2030*, p. 2. <https://seguridadvial2030.dgt.es/areas-estrategicas/vehiculos-seguros-y-conectados/>

tramos ante varias alternativas legales del posible marco regulatorio, donde debemos abordar si es preciso mantener o modificar la normativa actual de la legislación especial sobre responsabilidad civil y seguro en la circulación de vehículos a motor, incluso crear otra ex novo, y si la reciente normativa europea en materia de inteligencia artificial o sobre productos defectuosos ofrece soluciones aplicables a este escenario.

Para ello, el primer paso que vamos a abordar es el análisis del criterio de imputación de la responsabilidad aplicable en estos momentos al ámbito de los accidentes de circulación, y los hitos más relevantes que se han ido llevando a cabo en esta regulación, que será crucial en nuestras conclusiones. Para posteriormente tener en cuenta cómo afecta en la conducción autónoma y en sus distintos niveles de conducción la aplicación de esta normativa que se centra en la figura del conductor como responsable del manejo del vehículo. A continuación, nos detendremos en las propuestas regulatorias que se están llevando a cabo en materia de conducción autónoma. El estudio finalizará con un análisis de las nuevas normas europeas que van a afectar a este sector como es el Reglamento de Inteligencia Artificial, la próxima Directiva sobre responsabilidad por los daños causados productos defectuosos y la futura Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial.

2. EVOLUCIÓN Y REGULACIÓN DE LA RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL POR DAÑOS EN LA CIRCULACIÓN DE VEHÍCULOS A MOTOR

La responsabilidad derivada de la circulación de vehículos a motor es uno de los campos donde más ha evolucionado nuestro sistema de responsabilidad civil y lo seguirá haciendo, no solo por las reivindicaciones de una mayor protección a las víctimas, sino por el propio desarrollo de los vehículos que transitan en el parque automovilístico y cuyos avances tecnológicos van proporcionando un mayor nivel de conducción autónoma.

2.1. EVOLUCIÓN LEGAL DE LA RESPONSABILIDAD DERIVADA DE LOS ACCIDENTES DE CIRCULACIÓN

La evolución de la regulación legal de la circulación de vehículos a motor en nuestra carreteras da muestra de la relevancia de la materia y de cómo se ha ido adaptando al progreso. Si en sus albores se regía por el criterio general

del artículo 1902 del Código Civil, no fue hasta 1962 cuando se aprobó una ley especial sobre la materia, la cual fue evolucionando mediante la adopción de importantes modificaciones legislativas (cuyos hitos principales se produjeron en 1995, 2007 y 2015). A tal efecto, podemos distinguir las siguientes etapas en este cambio, que puede ayudarnos a comprender cómo se ha ido adaptando nuestro sistema de responsabilidad civil en el tráfico rodado a los dictados de los tiempos y a las necesidades de protección a las víctimas conforme a las directivas europeas³.

En un primer momento, hasta la aparición de una ley especial, la responsabilidad por la circulación de vehículos a motor se regía, como hemos avanzado, por el principio culpabilístico general establecido en los artículos 1902 y 1903 del Código Civil, recogiendo la herencia iusnaturalista y la máxima de «no responsabilidad sin culpa o dolo». Debido a la insuficiencia de este sistema de responsabilidad, asentado en la culpa, para proteger a las víctimas de los riesgos generado por el avance tecnológico e industrial, algunos ordenamientos jurídicos europeos fueron introduciendo un sistema de responsabilidad objetiva respecto a diversas actividades peligrosas, si bien la circulación de vehículos de motor no se erigirá inicialmente como tal, sino como un sistema intermedio, incrementando los niveles exigidos de conducta al conductor del vehículo a motor, quedando la teoría clásica de la culpa relegada a un segundo, aunque imprescindible, plano. En nuestro país, este cambio vino de la mano de la jurisprudencia que, aunque inicialmente exigía que para que se concediera una indemnización de daños y perjuicios era preciso demostrar la culpa o negligencia del demandado (SSTS de 15 de febrero de 1924 o de 29 de diciembre de 1939), años después, ante ese cambio tecnológico y el aumento de los riesgos derivados de los vehículos de motor (por lo tanto, atendiendo a la *realidad social del tiempo* en que las normas han de ser *aplicadas, conforme al* artículo 3.1 del Código Civil), efectúa una interpretación del artículo 1902 al enjuiciar estos supuestos. De este modo, a partir de mediados de los años cuarenta (STS de 10 de julio de 1943) da un giro a su tradicional pronunciamiento sobre este precepto mediante una serie de mecanismos como eran la presunción de culpabilidad del agente dañador, la inversión de la carga de la prueba y el incremento del deber de diligencia exigible, a través de la exigencia de una diligencia más alta que la del mero cumplimiento de disposiciones administrativamente regladas.

Hubo que esperar a la Ley 122/1962, de 24 de diciembre sobre Uso y Circulación de Vehículos de Motor (LUCVM) para consagrar un sistema pro-

³ Para un análisis más exhaustivo de esta evolución legislativa nos remitimos al estudio realizado en Monterroso Casado (2020). De la responsabilidad civil a la indemnización por daños derivados de la contribución causal al accidente de circulación. En López y García de la Serrana, J. (Dir.). *Responsabilidad civil y Seguro. Homenaje a Mariano Medina Crespo* Sepin, Madrid, pp. 813-848.

pio de esta responsabilidad. El Real Decreto Legislativo 1301/1986, de 28 de junio, de adaptación al ordenamiento jurídico comunitario supuso una nueva regulación para adecuar su contenido a dos Directivas del seguro de automóviles, que dieron como resultado la suscripción obligatoria de un seguro de responsabilidad civil cubriendo, en los términos y la extensión prevista en la normativa comunitaria, tanto los daños corporales como los materiales; y la revisión y ampliación de las funciones del Consorcio de Compensación de Seguros para reparar dichos daños. Bajo estas premisas, no es que se hubiera tenido que adaptar el régimen de responsabilidad civil, sino el sistema de cobertura. De este modo, se mantuvo el principio de responsabilidad objetiva atenuada para los daños corporales cubiertos por el seguro obligatorio, pero no se quiso incluir la responsabilidad por daños materiales, que se recondujo al criterio de atribución tradicional de la culpa.

La Ley 30/1995, de 8 de noviembre, de ordenación y supervisión de los seguros privados incorporó una tercera Directiva, que ampliaba en el sistema obligatorio de cobertura las responsabilidades derivadas de estos accidentes. Esta reforma afectó a la precisión de denominación de la ley, bajo el enunciado de Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor (LRCSCVM), y garantizaba que únicamente los daños personales sufridos por el conductor quedaban excluidos de la cobertura por el seguro obligatorio y la cobertura territorial del seguro obligatorio. El legislador recogía expresamente, por primera vez, en su articulado, el principio de la responsabilidad por riesgo como criterio de imputación de la responsabilidad, adquiriendo desde entonces un efecto vinculante. Y, a continuación, se establecían unas reglas de la carga de la prueba de ciertas circunstancias exoneradoras de esta responsabilidad objetiva del conductor y una remisión al artículo 1902 del CC en el supuesto en que acontecieran daños materiales. Asimismo, se manifestaba que la responsabilidad objetiva consagrada respecto a los daños personales se extendía no solo hasta el límite del seguro obligatorio. Por otro lado, mediante una disposición adicional, se incorporó un anexo con un «Sistema para la valoración de los daños y perjuicios causados a las personas en accidentes de circulación», en el que se recogía un sistema legal de delimitación cuantitativa del importe de las indemnizaciones exigibles por el daño causado a las personas, con independencia de la existencia o no de seguro y de sus límites cuantitativos.

El Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la LRCSCVM, para la adopción de una cuarta Directiva sobre el seguro de automóviles, exigió una nueva modificación para paliar las lagunas existentes en lo que se refiere a la liquidación de siniestros en los casos de accidentes de circulación ocurridos en un Estado miembro distinto al de residencia del perjudicado. También se aprovechó para recoger las consecuencias

de la declaración de inconstitucionalidad (STC 181/2000, de 29 de junio) del baremo relativas de la aplicación de ciertos factores de corrección.

La Ley 21/2007, de 11 de julio, que modificó el texto legal, fue fruto de una quinta Directiva, fundamentalmente en lo relativo a la configuración de la responsabilidad civil derivada de la circulación de vehículos a motor y el seguro que obligatoriamente la cubre, elevando las cuantías mínimas, definiendo el estacionamiento habitual del vehículo en España y obligando a las entidades aseguradoras a presentar una oferta motivada de indemnización en el caso de que se haya determinado la responsabilidad y se haya cuantificado el daño, o, en caso contrario, de una respuesta motivada a lo planteado en la reclamación. Además, se introdujo un nuevo apartado respecto a la responsabilidad del propietario del vehículo, no conductor, en el caso de ausencia de seguro de suscripción obligatoria.

El último avance vino de la mano de la Ley 35/2015, de 22 de septiembre, de reforma del sistema para la valoración de los daños y perjuicios causados a las personas en accidentes de circulación. No solo supuso una reforma y derogación integral del sistema vigente hasta la fecha para esa valoración, sino que se efectuó una modificación relevante en el criterio de imputación de la responsabilidad⁴. El legislador, aunque va a permanecer fiel al enunciado recogido en su texto del principio de responsabilidad por riesgo, va a proceder a modificar la moderación de la responsabilidad en los supuestos de concurrencia de culpa de la víctima. La imputación de la responsabilidad al conductor por el daño causado da paso a un nuevo escenario en el va ser posible prescindir de la propia causalidad, de manera que podemos afirmar que en la actual regulación jurídica conviven dos regímenes distintos que dan lugar a una indemnización de los daños causados por los accidentes de circulación. Por un lado, un sistema de imputación de la responsabilidad en virtud del riesgo y que, a su vez, establece un marco de regulación distinto en función de si acontecen daños en las personas o en los bienes. Por otro lado, un sistema de imputación del daño causado a determinadas víctimas, como veremos, prescindiendo del elemento causal y, por lo tanto, sin que dicha regulación constituya un régimen de responsabilidad, siendo más propio de la cobertura de un seguro de daños que de un seguro de responsabilidad civil.

⁴ La finalidad de Ley 35/2015, de 22 de septiembre, según recoge la propia Exposición de Motivos, es lograr la total indemnización de los daños y perjuicios para situar a la víctima en una posición lo más parecida posible a la que tendría de no haberse producido el accidente. Además, se modifican sustancialmente los principios rectores del sistema, los daños indemnizables, los sujetos beneficiarios, el modo de cálculo y las cuantías indemnizatorias del vigente sistema legal valorativo.

En definitiva, hasta la reforma de la Ley 35/2015 nos encontrábamos ante un principio de responsabilidad civil por riesgo que, si bien adolecía del elemento de la culpa, venía exigiendo una causalidad jurídica, requiriendo la existencia de un nexo causal entre el resultado dañoso y la conducta del agente dañador para poder imputar la responsabilidad. Actualmente, este sistema ha quedado deformado, al incorporar un modelo de indemnización que no corresponde a un sistema de responsabilidad civil ni a un sistema de indemnización por daños. Se trata de un mecanismo de indemnización sin culpa, donde la indemnización procede cuando no es posible la imputación de la responsabilidad a un sujeto sin capacidad de culpa civil o bien, en menor medida y con ciertos límites porcentuales, al tratarse de una víctima con dicha capacidad. Aunque podemos elogiar su incorporación al ordenamiento⁵, hay que reconocer que resulta contrario a nuestro actual sistema de responsabilidad civil, donde el aseguramiento obligatorio de los daños corporales debería estar sometido a las premisas de la responsabilidad civil, si se configura la mecánica de este seguro como tal. Por dicho motivo, podemos afirmar que el sistema instaurado por la Ley 30/2015 resulta incompatible con el mismo, por mucho que lo defienda y sea acorde con el criterio de solidaridad social y la protección jurídica de las víctimas.

En esta tesitura, lo correcto sería extender la aplicación de este criterio al operador o al propietario en el caso de vehículos de conducción autónoma que carezcan de conductor⁶. Pedimos al lector que preste atención a dicho modelo real actual, que se detalla a continuación, sin dejarse llevar por el enunciado del texto legal, ya que este aspecto será relevante a la hora de elaborar nuestra postura sobre el marco regulatorio del resarcimiento de daños causados por los vehículos autónomos.

2.2. REGULACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO DE LA RESPONSABILIDAD DERIVADA DE LOS ACCIDENTES DE CIRCULACIÓN

Nuestro sistema establece un criterio de imputación de la responsabilidad para el caso de los daños personales y daños materiales ocasionados en la circulación⁷. De este modo, una vez imputada la responsabilidad al conductor

⁵ Postura defendida desde mucho tiempo atrás con una propuesta de lege ferenda. Monterroso Casado, E. (2009). *Responsabilidad por accidentes de circulación. La concurrencia de causas*, Aranzadi, Navarra, p. 559.; y (2001), p. 386.

⁶ He tenido ocasión de ponerlo de relieve en Monterroso Casado (2020). De la responsabilidad civil a la indemnización por daños derivados de la contribución causal al accidente de circulación, op. cit., p. 822.

⁷ Monterroso Casado, E. (2020). *Responsabilidad civil derivada de los accidentes de circulación y valoración de daños a las personas conforme a la Ley 35/2015, de 22 de septiembre*, CEF, 4ª ed., Madrid.

del vehículo, en virtud del riesgo, por los daños causados a las personas o a los bienes, la LRCSCVM efectúa una matización entre daños materiales y personales. El artículo primero, apartado segundo, se refiere a daños a las personas, mientras que el apartado tercero contempla el supuesto de los daños materiales. Así lo recoge el artículo 1.1, párrafo segundo cuando señala que: “En el caso de daños a las personas, de esta responsabilidad solo quedará exonerado cuando pruebe que los daños fueron debidos a la culpa exclusiva del perjudicado o a fuerza mayor extraña a la conducción o al funcionamiento del vehículo; no se considerarán casos de fuerza mayor los defectos del vehículo ni la rotura o fallo de alguna de sus piezas o mecanismos”. Y el artículo 1.1, párrafo tercero, al disponer que: “En el caso de daños en los bienes, el conductor responderá frente a terceros cuando resulte civilmente responsable según lo establecido en los artículos 1902 y siguientes del CC, artículos 109 y siguientes del CP, y según lo dispuesto en esta Ley”.

De esta forma, aunque rige el principio del riesgo como criterio de imputación, tanto para los supuestos de daños corporales como materiales, respecto a los daños en las personas, el legislador establece una responsabilidad objetiva del conductor por dichos daños, quedando únicamente liberado por culpa exclusiva del perjudicado o fuerza mayor extraña a la conducción o al funcionamiento del vehículo. Esta responsabilidad objetiva respecto de los daños personales se extiende más allá del límite del seguro obligatorio (reformando la primitiva legislación). En cuanto a los daños materiales, la Ley establece la responsabilidad del conductor frente a terceros cuando resulte civilmente responsable a tenor de los preceptos señalados y, por tanto, ante una responsabilidad por culpa.

También es relevante hacer referencia a los efectos del riesgo de origen unilateral en la imputación de la responsabilidad (es decir, cuando intervienen, por ejemplo, el conductor de un vehículo y un peatón ajeno al riesgo, frente al riesgo bilateral en donde circulan dos conductores). En tales casos, si se aprecia la existencia de culpa de una víctima atropellada (peatón) es importante tener en cuenta que la ausencia de capacidad de culpa civil del sujeto, aunque con su conducta contribuyera al resultado, incide en la responsabilidad exigible al conductor. Por otro lado, se considera también que existe contribución al resultado, en el caso de la falta de uso o uso inadecuado de cinturones, casco u otros elementos protectores, incumpliendo la normativa de seguridad, si provoca la agravación del daño.

Por consiguiente, y de conformidad con el artículo 1.2 LRCSCVM, en el caso de que la víctima sea un peatón atropellado que posee capacidad de culpa civil (por ejemplo, un adulto con plenas facultades) y contribuye (por ejemplo, atraviesa la calzada por un lugar no destinado al efecto) a la producción

del daño, sea muerte o lesión, se podrá reducir su indemnización, en atención a la culpa concurrente, hasta un máximo del 75 % (incluso, aunque las circunstancias revelaran mayor causalidad). Sin embargo, no será posible exonerar de responsabilidad al conductor ni imputar alguna responsabilidad a la víctima por sus lesiones, si esta no es capaz de culpa civil, por tratarse de un menor de catorce años o que sufran un menoscabo físico, intelectual, sensorial u orgánico que afecta a la misma.

Una vez efectuadas estas distinciones, vamos a analizar si se pudiera extender su aplicación a los vehículos autónomos. En primer lugar, respecto al criterio de imputación de la responsabilidad en virtud del riesgo no parece que existan, en principio, inconvenientes para aplicar este criterio al propietario en el caso de un vehículo de conducción autónoma que carezca de conductor. Es más, aunque se haya comprobado que ese tipo de conducción sea más segura, no dejaría de considerarse como una actividad generadora de daños cubierta por un seguro obligatorio. En este sentido, Elizalde propone una reforma del artículo 1 de la LRCSCVM señalando la responsabilidad no solo del conductor, sino además del propietario del vehículo autónomo, considerando que, en el propio apartado, debería incluirse una definición de vehículo autónomo⁸. Sin embargo, en mi opinión, no debiera ir en ese lugar, al igual que tampoco se recoge una definición de vehículo a motor, sino que los conceptos de vehículo a motor, circulación de vehículos o hechos de la circulación a los efectos del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor se encuentran en los artículos 1 y 2 del Real Decreto 1507/2008, de 12 de septiembre, por el que se aprueba su Reglamento.

La segunda cuestión es la relativa a la distinción en el sistema de responsabilidad por accidentes de circulación entre daños personales y materiales. A este respecto, hemos de señalar que, incluso, en la conducción no autónoma, ya he tenido ocasión de manifestar que lo más acertado hubiera sido que no se estableciera esa dicotomía en la regulación de los daños personales y materiales causados a la hora de determinar la responsabilidad de cualquier daño derivado en la circulación de vehículos a motor y que, por lo tanto, existiera un único régimen de responsabilidad que eliminara cualquier posibilidad de que el caso fortuito eximiera de responsabilidad, incluso tratándose de daños materiales, y que, obviamente, los intereses del sector asegurador en este ámbito han podido constituir un lastre para el legislador⁹, que esperemos que

⁸ Elizalde Salazar, I (2022). *Vehículos autónomos. Responsabilidad civil y seguro*, Aranzadi, Pamplona, p. 143.

⁹ Monterroso, Casado, E. (2020). Responsabilidad civil derivada de los daños en los bienes causados por colisión recíproca de vehículos, *RCDI*, 781, p. 3191.

puedan corregirse en el futuro cuando acontezca una nueva regulación con ocasión de la regulación de la conducción autónoma.

Por otro lado, la mención legislativa sobre la fuerza mayor y la imposibilidad de considerar como tal los defectos del vehículo, al igual que la rotura o fallo de alguna de sus piezas o mecanismos, resulta también de utilidad práctica para la conducción autónoma de los vehículos en cualquier nivel para evitar la desprotección de la víctimas. Y, del mismo modo, podría resultar análogamente de aplicación como contribución causal, la regulación relativa a los supuestos de la falta de elementos o dispositivos de seguridad que pudieran provocar una agravación del daño, que podría incluso aplicarse a los casos en los que estos se hubieran desactivado, incumpliendo la normativa que dispusiera su uso obligatorio, y pudiera probarse que hubieran evitado o aminorado el daño.

Más controvertidos resultan los casos de daños personales por colisión recíproca sin determinación del grado o porcentaje de culpa de cada conductor en un escenario de conducción autónoma. Entiendo que el resultado debería ser el de la plena reparación de los daños causados al contrario, y que la indemnización solo quedaría excluida por culpa exclusiva de la víctima o fuerza mayor extraña a la conducción o al funcionamiento del vehículo, lo que equivale a una responsabilidad sin culpa del conductor u operador del vehículo. En tales casos, si no hay prueba del grado de culpa de cada conductor, ambos conductores responderían del total de los daños personales causados a los ocupantes del otro vehículo con arreglo a la doctrina de las indemnizaciones cruzadas¹⁰. Aunque este criterio no puede llegar a sostenerse respecto a los daños materiales con la actual legislación, que a efectos prácticos, y no sin pocas críticas al respecto, cada conductor debe ser el que asuma la indemnización de los daños del otro vehículo en un 50%¹¹, siendo deseable una reforma legislativa donde se acuda al criterio del resarcimiento cruzado de daños. De este modo, si se acometiera una regulación para ambos tipos de daños podría extenderse en la misma medida, y máxime cuando coexistan distintos vehículos con distintos niveles de automatización, al menos en las primeras fases.

¹⁰ La STS, de Pleno, de 10 de septiembre de 2012, resolviendo también un supuesto de colisión en el que no existía prueba del punto de impacto ni de qué vehículo fue el que invadió el carril contrario y, por lo tanto, no se podía saber si la culpa causalmente determinante del siniestro fue de uno u otro conductor, señala que el hecho de que no exista prueba sobre la culpa del conductor no incide en el criterio de imputación de la responsabilidad que se basa en el riesgo y, en consecuencia, sin que una recíproca colisión de vehículos suponga una excepción a la aplicación del principio de responsabilidad objetiva por el riesgo de la circulación.

¹¹ Interpretación que señala como más adecuada el Tribunal Supremo, Sala de lo Civil, en sentencia de Pleno de 27 de mayo de 2019.

Tampoco debe obviarse la protección de forma especial a los sujetos sin capacidad civil, es decir, los supuestos en los que exista una concurrencia o una exclusiva culpa de la víctima no conductora que es menor de 14 años o es un discapacitado (entendido como sujeto que sufra un menoscabo físico, intelectual, sensorial u orgánico que le prive de capacidad de culpa civil) ya que no se suprime ni se reduce la indemnización en caso de que padezca secuelas y lesiones, salvo en el caso de contribución dolosa. Ni tampoco se permite la acción de repetición contra los padres y tutores, y demás personas físicas que, en su caso, deban responder por ellas legalmente. Por otro lado, el legislador posibilita que en los demás supuestos (es decir, cuando las víctimas hayan cumplido los 15 años o sean capaces de culpa civil) pueda existir culpa exclusiva o concurrencia de culpas, pero limitando, en este último caso, la reducción de la indemnización hasta un máximo del 75%, por lo que no se toma en consideración si su grado de contribución al daño ha sido superior a dicho porcentaje causal. Ahora bien, aunque este sistema legal resulta encomiable por la mayor protección que concede a las víctimas es incompatible con el sistema tradicional de la responsabilidad civil, que exige de una causalidad jurídica para imputar la responsabilidad, por mucho que lo consideremos acorde con el criterio de solidaridad social y protección jurídica de las víctimas. Nos encontramos ante un mecanismo de indemnización sin culpa en aquellos casos en los que se establece una indemnización aunque no exista un nexo causal entre el resultado dañoso y la conducta del agente dañador¹². Por lo tanto, el escenario actual del sistema de responsabilidad civil en el ámbito de la circulación de vehículos a motor ha quedado desfigurado, al incorporar a nuestro ordenamiento, un modelo de indemnización que no obedece claramente ni a un sistema de responsabilidad ni a un sistema de indemnización por daños, lo que facilita, a fin de cuentas, que pueda también extenderse a la nueva realidad de circulación autónoma de vehículos donde el concepto de negligencia imputable a un sujeto concreto irá disminuyendo o, incluso, será en muchos casos imposible de determinar. Por este motivo, considero que no es preciso delimitar los tipos de responsabilidades en función de los niveles de automatización¹³, sino aplicar un sistema uniforme de indemnización sin per-

¹² Monterroso Casado, E., Responsabilidad civil derivada de los daños en los bienes causados por colisión recíproca, op. cit., p. 3191.

¹³ Elizalde Salazar establece una distintas reglas de responsabilidad en función de los distintos niveles de autonomía, señalando que para los niveles 2 y 3 las reglas de responsabilidad que establece la LRCSCVM no precisarían de reforma legal alguna para que resultasen de aplicación a estos vehículos (*Vehículos autónomos. Responsabilidad civil y seguro*, op. cit., pp. 104-109). Sin embargo, para el nivel 4, en el que no se necesita la supervisión de la conducción por el conductor, aunque se precisa que exista una un sujeto en su interior que pueda tomar el control, si el sistema autónomo está desactivado se aplicarían las reglas de la LRCSCVM, aunque no aparece la alternativa de cuando se encuentre activo el sistema (pp. 115-116).

juicio de las facultades de repetición contra terceros. No se trata de imputar la responsabilidad tomando como fundamento el deber de control sobre el vehículo autónomo, como sucede con otros robots, ya que su propia autonomía podría imposibilitar la misma, sino que se debe tomar en consideración su ámbito de aplicación, en el que existen unos mecanismos de protección a las víctimas por accidentes de circulación fruto de una necesidad social y que cuenta con un seguro obligatorio, cuyas primas son abonadas por los propietarios de los vehículos.

Dicho esto y para poder abordar posibles soluciones, tendremos que analizar las características de los vehículos autónomos, sus niveles de autonomía y el estado actual de implantación de estos vehículos, la normativa existente relativa a la homologación para su circulación y las propuestas de desarrollo de las normas de circulación autónoma. A continuación, consideramos preciso examinar también las últimas disposiciones europeas en materia de inteligencia artificial, productos defectuosos y responsabilidad en materia de IA para poder determinar cómo pueden confluir en la responsabilidad civil del tráfico rodado.

3. VEHÍCULOS AUTÓNOMOS Y CONDUCCIÓN AUTOMATIZADA

3.1. EL VEHÍCULO AUTÓNOMO

Son varios los términos que se vienen utilizando en relación al vehículo autónomo, vehículo automatizado, vehículo sin conductor, vehículo inteligente, vehículo conectado, vehículo asistido, vehículo autopilotado. Estos conceptos se aplican a distintos niveles de conducción autónoma que requieren de un entorno dotado de IA. De hecho, el punto más relevante es que no se limita al control del volante, sino que detecta el entorno donde transita, captando información desde el exterior y, en base al análisis que realiza, aplica el modo de conducción más conveniente, como puede ser identificar una ruta, medir distancias, identificar carriles y calzada, monitorizar otros vehículos y peatones, o reconocer obstáculos y señales de tráfico.

El que un vehículo cuente con dispositivos de IA no implica necesariamente que se considere autónomo, ya que dependerá de la intervención humana a cargo del mismo. Asimismo, para que circule sin intervención del conductor, además de requerir de una serie de características técnicas como sensores de radares y cámaras o sistemas de posicionamiento, entre muchos otros, es preciso que se intercomunique o, dicho de otro modo, se encuentre

conectado con el entorno para que transmita y reciba información de la vía, del tráfico o de otros usuarios, y que un software procese toda la información, enviando instrucciones sobre el acelerado, el frenado y la dirección. La autonomía total permitirá, incluso, que los sistemas puedan ir aprendiendo, y generando nuevos patrones de respuesta, ante infinitudes distintas de escenarios y circunstancias que puedan darse en la conducción.

El Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, distingue entre las definiciones de vehículo automatizado y de vehículo totalmente automatizado, en función de si se requiere al conductor su intervención. De este modo, establece como «vehículo automatizado»: un vehículo de motor diseñado y construido para desplazarse de manera autónoma durante determinados períodos de tiempo sin supervisión continuada por parte del conductor pero respecto del cual se sigue esperando o necesitando la intervención del conductor; y como «vehículo totalmente automatizado»: un vehículo de motor diseñado y construido para desplazarse de manera autónoma sin supervisión por parte del conductor.

Estos vehículos de conducción automatizada utilizan diferentes tecnologías de sistemas avanzados de asistencia al conductor (ADAS) como los sensores de percepción del entorno (láser, radar, sensores ultrasónicos, TracePro, LiDAR, infrarrojos, visión computerizada por cámara), sistemas de posicionamiento (GPS), sistemas de comunicaciones, vehículos conectados (V2V y V2I), sistemas avanzados de control, así como *edge computing*, para un ultra rápido procesamiento de datos en tiempo real, para ejecutar el software y transformar los datos recabados por los sensores en acciones concretas sobre la conducción.

Con esta tecnología, procesada por un software para percibir al entorno, se crean unas tareas de conducción dinámicas (*Dinamic Driving Tasks*, DDT), como son: OEDR -*Object and Event Detection and Response* (a través de la detección y respuesta ante objetos y eventos se definen las tareas de monitorizar el entorno y ejecutar una respuesta)¹⁴, ODD -*Operational Design Domain* (el dominio de diseño operativo es un término para un contexto operativo, incluyendo las condiciones ambientales, geográficas, hora y estado del tráfico)¹⁵, o el DDT *fallback* (respuesta del usuario o del sistemas tras un fallo,

¹⁴ *Object and event detection and response*. <https://taxonomy.connectedautomateddriving.eu/object-and-event-detection-and-response/>

¹⁵ *What Are Operational Design Domains?*. <https://www.apativ.com/en/insights/article/what-are-operational-design-domains>

al salir del dominio de diseño operativo, para minimizar el riesgo dadas las circunstancias)¹⁶. La utilización de estas tecnologías incide en la clasificación de los niveles de autonomía de un vehículo que veremos a continuación y, por lo tanto, en las capacidades de conducción sin intervención del conductor.

3.2. LOS NIVELES DE AUTONOMÍA

Distintos organismos estipulan diferentes clasificaciones en los niveles de conducción, siendo los establecidos por la SAE y la NHTSA los de mayor reconocimiento. La SAE, *Society of Automotive Engineers*, se creó en EEUU en 1905, para promover el uso de los estándares de los automóviles¹⁷. La NHTSA, *National Highway Traffic Safety Administration*, es la agencia federal de EEUU encargada de velar por la seguridad en la circulación de vehículos¹⁸ y fue el primer organismo que, en 2013, efectuó una clasificación de los distintos niveles de conducción autónoma. Si bien debido a que la falta de uniformidad generaba una ineficiencia a la hora de indicar el grado de autonomía debido a la coexistencia de diferentes escalas de conducción autónoma, se ha adoptado como estándar la categorización creada por la SAE, que es la que analizaremos. En nuestro país, la Dirección General de Tráfico acoge ese modelo de niveles de conducción autónoma, del que se ha ido aprobando distintas versiones desde 2014.

Los estándares de conducción autónoma realizados por la SAE se clasifican en seis niveles de automatización, que comprenden tres grandes bloques: nada o poco automatizado, parcialmente automatizado y altamente automatizado. En el primer bloque estaría el nivel 0 «Conducción manual», en el que el conductor se encarga de la conducción sin ayuda sin ningún sistema

¹⁶ *DDT fallback*: <https://www.lawinsider.com/dictionary/ddt-fallback>

¹⁷ SAE, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, https://www.sae.org/standards/content/j3016_202104/ (última versión J3016_202104)

¹⁸ La NHTSA clasifica los distintos niveles de conducción autónoma del siguiente modo: Nivel 0: Asistencia momentánea al conductor; Nivel 1 Asistencia al conductor; Nivel 2: Asistencia adicional; Nivel 3: Automatización condicional; Nivel 4: Alta automatización; y Nivel 5: Automatización completa. En el nivel 4, el sistema cuando está activado (ya que permite ambos sistemas de conducción, el del conductor y el del propio sistema) es totalmente responsable de las tareas de conducción dentro de áreas de servicio limitadas, es decir, no en cualquier espacio. Y en el último sistema añadido, el de “Full Automation”, el vehículo puede conducir completamente por sí solo, sin necesidad de asistencia humana, siendo el sistema totalmente responsable de las tareas de conducción, mientras que los ocupantes actúan solo como pasajeros y no necesitan participar en la conducción. En <https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety> se pueden consultar “Automated Vehicles for Safety”.

de ayuda¹⁹, y el nivel 1 «Conducción asistida», en el que un sistema de asistencia controla la dirección o la aceleración/desaceleración, nunca los dos, y el conductor realiza las demás funciones relativas a la conducción. En el segundo bloque, es decir, el parcialmente automatizado estaría el nivel 2 «Automatización parcial», en el que varios sistemas de asistencia a la conducción se encargan de estas funciones de dirección y de aceleración/desaceleración, y el conductor debe seguir atento y llevar a cabo el resto de tareas, y el nivel 3, que sería el de «Automatización condicionada», en el que el sistema realiza todas las tareas de conducción, pero con limitaciones ya que el conductor debe responder a cualquier solicitud de intervención por parte del sistema. El tercer bloque sería el altamente automatizado, donde se ubicaría el nivel 4 «Automatización alta», en el que el sistema realiza todas las tareas de conducción incluso aunque el conductor humano no responda a una solicitud de intervención y, por último, estaría el nivel 5 de «Automatización total», que se trataría de un sistema de conducción automatizada que realiza todas las tareas de conducción en cualquier condición, por lo que el vehículo puede prescindir del conductor²⁰.

Como podemos observar, en los supuestos de conducción autónoma de nivel 1 o de nivel 2, el conductor siempre tiene el control del vehículo, mientras que en el nivel 3 el conductor debe intervenir si es necesario, recibiendo un aviso de que tome el control. De hecho, hasta el nivel 2, incluido, realmente son sistemas de asistencia a la conducción del vehículo y el nivel máximo de automatización que se permite circular por nuestras carreteras. El siguiente paso es el nivel 3, en el que el conductor tiene que estar preparado para tomar el control del vehículo en caso de aviso, y el nivel 4 que ya no precisa del conductor al tener capacidad para efectuar cualquier función de la conducción en determinadas condiciones (si fuera en todas las condiciones ya nos encontraríamos ante un nivel 5 de automatización completa).

Aunque la tecnología ya permite una conducción totalmente autónoma, en la actualidad, no existe un coche de conducción completamente

¹⁹ Señala la SAE que los sistemas de seguridad activa, como el control electrónico de estabilidad (ESC) y el frenado automático de emergencia (AEB), y ciertos tipos de sistemas de asistencia al conductor, como el asistente de mantenimiento de carril (LKA), están excluidos del alcance de esta clasificación de automatización de la conducción porque no realizan parte o la totalidad de la DDT de manera sostenida, sino que posibilitan una intervención momentánea durante situaciones potencialmente peligrosas. Debido a la naturaleza momentánea de las acciones de los sistemas de seguridad activa, su intervención no cambia ni elimina el rol del conductor en la realización de parte o la totalidad de la DDT y, por lo tanto, no se consideran automatización de la conducción, aunque realicen funciones automatizadas ((Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, cit.).

²⁰ DGT, Vehículos de conducción automatizada, <https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/vehiculos-de-conduccion-automatizada/>

autónomo que se comercialice en el mercado, con independencia de prototipos de prueba. El marco normativo actual de España no posibilita la circulación en el nivel 3 o superior, por lo tanto, no se permite que el conductor suelte el volante durante la conducción. Si bien, países europeos como Francia y Alemania ya disponen de una regulación que permite bajo ciertas y estrictas condiciones la circulación en ese tercer nivel de autonomía²¹.

3.3. AUTONOMÍA REAL EN LA OFERTA DE CONDUCCIÓN AUTOMATIZADA

Respecto a la autonomía real de vehículos comercializados, el nivel 1 es ya común encontrarlo en la oferta de los nuevos vehículos, como es el caso de aquellos con el sistema de velocidad adaptada, si bien, en la actualidad la mayoría de los modelos de turismos comercializados en España cuentan con un nivel de autonomía SAE 2 (75 % de los modelos), siendo la tecnología más incorporada la de los siguientes sistemas²²:

- Sistema de control de la presión de los neumáticos. TPMS - *Tyre Pressure Monitoring System*.
- Sistema Avanzado de Frenado de Emergencia. AEB – *Advanced Emergency Braking*.
- Sistema de advertencia de abandono de carril. LDW – *Lane Departure Warning*.
- Sistema de información sobre ángulos muertos. *Blind Spot Information System*.
- Llamada de emergencia (*e-Call*).
- Señal de frenado de emergencia. *Emergency Stop Signal*.
- Detector de marcha atrás. *Reversing detection*.
- Advertencia de colisión con peatones y ciclistas. *Pedestrian and cyclist collision warning*.
- Sistema de emergencia de mantenimiento del carril. ELKS – *Emergency Lane-keeping system*.

²¹ ANFAC, *Barómetro sobre vehículo autónomo y conectado*, <https://anfac.com/publicaciones/barometro-de-vehiculo-autonomo-y-conectado-edicion-2023/>, p. 30.

²² “Glosario de funcionalidades de autonomía”, en ANFAC, op. cit., pp. 6- 7. Mientras que la oferta automovilística actual, aunque el nivel de autonomía real para los turismos es mayoritariamente de SAE 2, en un 75% de los modelos, respecto a los vehículos comerciales ligeros cuenta con un nivel de autonomía SAE 1 solo el 49% de los modelos.

- Asistente de Velocidad Inteligente. ISA - *Intelligent Speed Assistance*.

En nuestro país, como hemos apuntado, solo se comercializan sistemas de conducción semiautónoma que serían de nivel 1 y 2, que permiten, por ejemplo, ajustar la velocidad o la dirección del vehículo para que se mantenga en el carril, o efectuar maniobras de aparcamiento, debiendo de estar el conductor disponible para intervenir y con las manos al volante para mantener su control si fuera preciso. Ahora bien, los fabricantes ya disponen de vehículos que superan los límites impuestos por la regulación actual. De hecho, se han incorporado nuevas funciones que podrían superar el SAE 2, aunque limitando el software, en algunos casos, para que no pueda considerarse un nivel SAE 3. Quizás el vehículo autónomo más conocido es el que opera con el sistema Autopilot del fabricante TESLA²³, aunque el avanzado software de FSD, con un nivel 3 SAE, resulta inutilizable según su diseño, en España y otros países de la UE, por lo que el fabricante ha comercializado una versión modificada del software (FSD Beta, y no el FSD V12)²⁴, lo que ha obligado al fabricante a modificar este sistema de piloto automático, si bien la compañía ha anunciado que llegará a Europa en 2025²⁵. También podemos mencionar el sistema de conducción autónoma Ford BlueCruise, que funciona con conducción asistida de manos libres nivel 2 en una Blue Zone²⁶; BMW, en su nuevo Serie 7, ha recibido aprobación en Alemania para una combinación de un sistema de asistencia de conducción de nivel 2 (el BMW Highway Assistant) y un sistema de nivel 3 en la forma del BMW Personal Pilot L3, que permite delegar completamente la tarea de conducir bajo ciertas condiciones²⁷; o Mercedes-Benz que ha lanzado el Drive Pilot en Estados Unidos (en

²³ https://www.tesla.com/es_es/support/autopilot

²⁴ Tesla, Piloto automático y Capacidad de conducción autónoma total, https://www.tesla.com/es_es/support/autopilot

²⁵ La cuenta oficial de AI de Tesla publicó en la red social X que el producto de asistencia FSD llegaría a Europa en el primer trimestre de 2025; ahora bien, no es la primera vez que la compañía ofrece expectativas que no ha podido cumplir. Euronews, “Tesla says ‘Full Self Driving’ cars expected in Europe early next year pending regulatory approval” .<https://www.euronews.com/next/2024/09/05/tesla-says-full-self-driving-car-expected-in-europe-early-next-year-pending-regulatory-app> (publicado el 5 de septiembre de 2024).

²⁶ Ford BlueCruiser: “Cuando se active, la función Ford BlueCruise controlará la dirección, la aceleración y el frenado del vehículo con la supervisión del conductor, y estará lista para intervenir en secciones precalificadas de las autopistas divididas pertinentes, llamadas Blue Zones “manos libres”, mientras la atención del conductor se centra en la carretera”. <https://www.ford.es/tecnologia/asistencia-conduccion/ford-bluecruise>

²⁷ BMW Group, BMW es el primer fabricante de automóviles en recibir aprobación para la combinación de conducción autónoma Nivel 2 y Nivel 3, 2 de julio de 2024 <https://www.press.bmw-group.com/spain/article/detail/T0443527ES/bmw-es-el-primer-fabricante-de-autom%C3%B3viles-en-recibir-aprobaci%C3%B3n-para-la-combinaci%C3%B3n-de-conducci%C3%B3n-aut%C3%B3noma-nivel-2-y-nivel-3?language=es>

California y Nevada) y Alemania (en tramos apropiados), siendo el primer sistema certificado nivel 3 SAE de conducción automatizada condicional²⁸.

Para que un vehículo circule sin la intervención del conductor es preciso no solo que se encuentre equipado de la tecnología precisa, sino que se intercomunique con el entorno y con otros usuarios, además de que la infraestructura vial pueda intercambiar información sobre la vía y el tráfico, es decir, se requiere de un entorno de IA, y es obvio que las carreteras, al menos las españolas, aún no están preparadas para albergar un vehículo de un nivel alto de autonomía. De este modo, debido a cuestiones de adaptación de la infraestructura y de adecuación de las vías, de intercomunicación de datos, así como por cuestiones morales y regulatorias, no se espera que la implantación generalizada de los vehículos completamente automatizados se produzca antes del 2030 (más allá de la Estrategia de Seguridad Vial 2030). No obstante, es preciso adaptar progresivamente la normativa a estos cambios, a medida que se pretende ir implantando esa primera fase de conducción parcialmente automatizada. En este sentido, señala la DGT que, "se debe poder asegurar que un vehículo autónomo es capaz de circular adoptando las mismas obligaciones y responsabilidades legales y el mismo nivel de cumplimiento del Reglamento General de Circulación que un vehículo con conductor, de forma que pueda compartir las vías públicas con seguridad, tanto para sus ocupantes como para el resto de personas usuarias, especialmente las más vulnerables"²⁹. A continuación, analizaremos la regulación específica que ha sido aprobada o que se está desarrollando respecto a este tipo de vehículos.

4. REGULACIÓN DE LA CONDUCCIÓN AUTOMATIZADA

4.1. MARCO JURÍDICO EUROPEO DE VEHÍCULOS AUTOMATIZADOS Y TOTALMENTE AUTOMATIZADOS

El primer marco jurídico de la UE para los vehículos automatizados y totalmente automatizados fue aprobado por el Reglamento (UE) 2019/2144 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad

²⁸ Mercedes Benz, Drive Pilot, https://www.mercedes-benz.es/passengercars/technology/drivepilot.html?srsId=AfmBOoqQ_TU3YGd05qMo68PxFzoWy6ZWNoyqn4pkBJXIIQMjCxcwYar9D (fecha consulta 10 septiembre 2024).

²⁹ DGT (2024). Vehículos seguros y conectados. *Estrategia de Seguridad Vial 2030*, cit., p. 213.

general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, que modifica el Reglamento (UE) 2018/858, y que se encuentra en vigor desde el 6 de julio de 2022. Uno de los principales objetivos de este Reglamento es reducir de manera significativa las muertes y lesiones graves en las carreteras de la Unión Europea mediante la introducción de tecnologías de seguridad de vanguardia³⁰. De hecho, en el Considerando décimo se pone de relieve que los sistemas de seguridad, que constituyen la base de tecnologías que también se utilizarán en la implantación de vehículos automatizado, tienen un elevado potencial de reducción de las cifras de víctimas de accidentes, y que, por lo tanto, deben establecerse normas armonizadas y procedimientos de ensayo para la homologación de estos vehículos y de tales sistemas como unidades técnicas independientes; asimismo debe garantizarse que estos sistemas puedan utilizarse de forma segura durante toda la vida útil del vehículo. Además, el progreso tecnológico de esos sistemas debe tenerse en cuenta en la legislación vigente para que tengan aplicación futura a fin de reducir o eliminar accidentes y lesiones en el transporte por carretera, respetando, por otro lado, la intimidad y la protección de datos. Resulta también interesante su considerando undécimo, que insta a que exista la posibilidad de desactivar el asistente de velocidad inteligente, que debe quedar bajo control del conductor (por ejemplo, cuando el conductor reciba advertencias falsas o información inadecuada como consecuencia de las inclemencias del tiempo, de indicaciones viales provisionales contradictorias en los tramos de obras, o de señalización vial confusa, defectuosa o inexistente).

Bajo esas premisas, para todos los vehículos nuevos, establece la obligación de que estén equipados con los siguientes sistemas avanzados de seguridad: asistente de velocidad inteligente; interfaz para la instalación de alcoholímetros antiarranque; sistema de advertencia de somnolencia y pérdida de atención del conductor; sistema avanzado de advertencia de distracciones del conductor; señal de frenado de emergencia; detector de marcha atrás; y registrador de datos de incidencias (artículo 6). Y, además, los turismos y las furgonetas deben de estar equipados con medidas de seguridad más avanzadas, incluidos: sistemas avanzados de frenado de emergencia, capaces de detectar los vehículos de motor y los usuarios vulnerables de la vía pública que van delante; sistemas de emergencia de mantenimiento del carril; una zona ampliada de protección frente a impactos en la cabeza capaz de mitigar las lesiones en colisiones con usuarios vulnerables de la vía pública (artículo 7). Ahora bien, estos sistemas no constituyen automatización, es decir, conducción autónoma.

³⁰ El Reglamento (UE) 2019/2144 establece los sistemas de seguridad que serán obligatorios en los vehículos de nueva homologación en toda Europa. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019R2144>

El artículo 11 sí establece unos requisitos específicos relativos a los vehículos automatizados y los vehículos totalmente automatizados, señalando que deben cumplir, además de los requisitos anteriores, con las especificaciones técnicas establecidas en los actos de ejecución relativas a: sistemas para sustituir el control del vehículo ejercido por el conductor, incluidos los de señalización, dirección, aceleración y frenado; sistemas para facilitar al vehículo información en tiempo real sobre su estado y el de la zona circundante; sistemas de monitorización de la disponibilidad del conductor; registradores de datos de incidencias para vehículos automatizados; formato armonizado de intercambio de datos en caso, por ejemplo, de formación de un pelotón de vehículos multimarca; y sistemas para proporcionar información relativa a la seguridad a otros usuarios de la vía.

Además, se apremia a la Comisión para que adopte, mediante actos de ejecución, disposiciones relativas a procedimientos y especificaciones técnicas para estos sistemas y elementos, y para la homologación de los vehículos automatizados y los vehículos totalmente automatizados en relación con los mismos para garantizar un funcionamiento seguro. También se prevé la revisión, debiendo presentar la Comisión un informe de evaluación de la eficacia de las medidas y sistemas de seguridad a más tardar el 7 de julio de 2027 (y posteriormente cada cinco años), que incluya, si es preciso, recomendaciones e incluir una propuesta legislativa con el fin de reducir, o eliminar, los accidentes y lesiones en el transporte por carretera.

Derivada de dicha facultad, la Comisión ha adoptado varios actos de ejecución y actos delegados. Respecto a los de ejecución, el Reglamento de Ejecución (UE) 2021/535 relativo a los procedimientos uniformes y las especificaciones técnicas para la homologación de tipo de los vehículos y de los sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, en lo que respecta a sus características generales de construcción y seguridad³¹; el Reglamento de Ejecución (UE) 2021/646 en cuanto a los procedimientos uniformes y las especificaciones técnicas para la homologación de tipo de los vehículos de motor con respecto a sus sistemas de emergencia de mantenimiento del carril³²; el Reglamento de Ejecución (UE) 2022/1426 de la Comisión de 5 de agosto de 2022 por el que se establecen normas para la aplicación del Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo en cuanto a los procedimientos uniformes y las especificaciones técnicas para la homologación de tipo del sistema de conduc-

³¹ Reglamento de Ejecución (UE) 2021/535. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32021R0535>

³² Reglamento de Ejecución (UE) 2021/646. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32021R0646>

ción automatizada (ADS) de los vehículos totalmente automatizados³³, o el Reglamento de Ejecución (UE) 2024/1721 de la Comisión, de 19 de junio de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo relativas a los modelos para la homologación del sistema de asistente de velocidad inteligente, el sistema de advertencia de somnolencia y pérdida de atención del conductor, el registrador de datos de incidencias, la interfaz para la instalación de alcoholímetros antiarranque y el sistema avanzado de advertencia de distracciones del conductor³⁴.

Los actos delegados se han realizado mediante la aprobación del Reglamento Delegado (UE) 2021/1243 con disposiciones de aplicación sobre la interfaz para la instalación de alcoholímetros antiarranque en los vehículos de motor y por el que se modifica el anexo II de dicho Reglamento³⁵; el Reglamento Delegado (UE) 2021/1341 por el que se establecen normas detalladas sobre los procedimientos de ensayo y los requisitos técnicos específicos por lo que respecta a sus sistemas de advertencia de somnolencia y pérdida de atención del conductor³⁶; el Reglamento Delegado (UE) 2021/1958 por el que se completa el Reglamento (UE) 2019/2144 con normas detalladas sobre los procedimientos de ensayo y los requisitos técnicos específicos para la homologación de tipo de los vehículos de motor en lo que respecta a sus sistemas de asistente de velocidad inteligente y para la homologación de tipo de tales sistemas como unidades técnicas independientes³⁷; el Reglamento Delegado (UE) 2022/545 por el que se completa el Reglamento (UE) 2019/2144 con normas detalladas sobre los procedimientos de ensayo y los requisitos técnicos específicos para la homologación de tipo de los vehículos de motor en lo que respecta a su registrador de datos de incidencias y para la homologación de tipo de tales sistemas como unidades técnicas independientes³⁸; el Reglamento Delegado (UE) 2022/1398 de la Comisión, de 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2019/2144 para tener en cuenta los avances técnicos y normativos relativos a las modificaciones de la reglamentación so-

³³ Reglamento de Ejecución (UE) 2022/1426. <https://eur-lex.europa.eu/eli/reg/2022/1426/spa>

³⁴ Reglamento de Ejecución (UE) 2024/1721. https://eur-lex.europa.eu/eli/reg_impl/2024/1721/spa

³⁵ Reglamento Delegado (UE) 2021/1243. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32021R1243>

³⁶ Reglamento Delegado (UE) 2021/1341. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32021R1341>

³⁷ Reglamento Delegado (UE) 2021/1958. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32021R1958>

³⁸ Reglamento Delegado (UE) 2022/545. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R0545>

bre vehículos adoptadas en el marco de la Comisión Económica para Europa de las Naciones Unidas³⁹; el Reglamento Delegado (UE) 2022/2236 de la Comisión de 20 de junio de 2022 por el que se modifican los anexos I, II, IV y V del Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos técnicos para los vehículos fabricados en series ilimitadas, los vehículos fabricados en series cortas, los vehículos totalmente automatizados fabricados en series cortas y los vehículos especiales, y en lo que respecta a las actualizaciones de software⁴⁰; o el Reglamento Delegado (UE) 2023/2590 de la Comisión, de 13 de julio de 2023, por el que se completa el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo mediante el establecimiento de normas de desarrollo relativas a los procedimientos de ensayo y los requisitos técnicos específicos para la homologación de tipo de determinados vehículos de motor en lo que respecta a sus sistemas avanzados de advertencia de distracciones del conductor, y por el que se modifica dicho Reglamento⁴¹.

Por último, también debemos hacer mención al Reglamento de Inteligencia Artificial, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, que, como veremos en su análisis modifica expresamente el Reglamento (UE) 2019/2144.

Las próximas líneas de actuación consisten en una modificación en la normativa sobre seguridad de los vehículos por la Comisión Europea, facultada para completar el marco legal para los vehículos automatizados, con el objeto de tratar de alinear la legislación de la UE con las nuevas reglas de la ONU sobre automatización de nivel 3, de modo que se tiene previsto adoptar nuevas normas técnicas para los vehículos automatizados que sustituyen al conductor en las autopistas (automatización de nivel 3) y los vehículos sin conductor en transbordadores o robotaxis (nivel 4)⁴². De este modo, se está avanzando en esta normativa a través de la elaboración de reglamentación de la Comisión Económica para Europa de las Naciones Unidas (CEPE) sobre Sistemas de Asistencia al Control de Conductor (*Driver Control Assist Systems*, DCAS) como, por ejemplo, el mantenimiento y el cambio de carril. Esta nue-

³⁹ Reglamento Delegado (UE) 2022/1398. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R1398>

⁴⁰ Reglamento Delegado (UE) 2022/2236. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2236>

⁴¹ Reglamento Delegado (UE) 2023/2590. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202302590

⁴² EsMartCity.es, Nuevo reglamento que establece en la UE el marco legal para vehículos automatizados y autónomos, *Movilidad Urbana*, 8 de julio de 2022. <https://www.esmartcity.es/2022/07/08/nuevo-reglamento-establece-ue-marco-legal-vehiculos-automatizados-autonomos>

va regulación está basada en su Reglamento n° 79⁴³. El nuevo reglamento de la CEPE no prevé la automatización total en la conducción y, por lo tanto, exige las siguientes medidas: que los fabricantes implementen estrategias para garantizar que los conductores tengan un conocimiento adecuado de las capacidades de los sistemas de asistencia y no las sobreestimen (la llamada *mode awareness*), que los DCAS deban diseñarse para garantizar que el conductor permanezca comprometido con la tarea de conducción, y que los fabricantes elaboren informes anuales del rendimiento de estos sistemas e incidentes relevantes⁴⁴. Dicho reglamento va a ser presentado en el Foro Mundial para la Armonización de Reglamentos de Vehículos (WP.29), organizado al amparo de la División de Transporte Sostenible de la CEPE⁴⁵, plataforma intergubernamental responsable de los marcos regulatorios relacionados con la seguridad, cuyo objetivo es crear un Reglamento de las Naciones Unidas para el diseño de vehículos en el comercio internacional. Debido a que los Reglamentos de la ONU entran en vigor seis meses después de su adopción por el Foro Mundial, está previsto para 2025. Es importante destacar también que respecto a la ciberseguridad de los vehículos automatizados, que comprenden desde los ADAS a las infraestructuras que lo posibilitan (sistemas ITS, plataforma DGT 3.0 o sistemas de gestión del tráfico)⁴⁶, ya existe una normativa, el Reglamento n° 155 de la CEPE relativo a la homologación de los vehículos de motor en cuanto a ciberseguridad y al sistema de gestión de esta (2021/387)⁴⁷, que exige que los vehículos que se homologuen cuenten con un certificado que acredite que están protegidos frente a ciberataques.

4.2. MARCO JURÍDICO NACIONAL DE CONDUCCIÓN AUTOMATIZADA

Conforme a la normativa europea, la regulación de los vehículos autónomos se está llevando a cabo por los Estados miembros, al ser los que deben regular el vehículo automatizado en su territorio, por un lado, en cuanto a los requisitos

⁴³ Reglamento n° 79 de la Comisión Económica para Europa de las Naciones Unidas (CEPE). Prescripciones uniformes relativas a la homologación de vehículos por lo que respecta al mecanismo de dirección [2018/1947]. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-82045>.

⁴⁴ El Grupo de Trabajo de la CEPE sobre Vehículos Automatizados/ Autónomos y Conectados (Working Party on Automated/Autonomous and Connected Vehicles, conocido por las siglas GRVA) ha elaborado un borrador de un nuevo reglamento que define disposiciones sobre DCAS y proporciona requisitos mínimos de ADAS. United Nations Economic Commission for Europe (UNECE). *New UN regulation paves the way for the roll-out of additional driver assistance systems*, <https://unece.org/media/press/387961>.

⁴⁵ Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (WP.29)-Funcionamiento- Participación. <https://unece.org/es/transport/publications/unidasforo-mundial-para-la-armonizacion-de-la-reglamentacion-sobre-vehiculos>

⁴⁶ DGT (2024). Vehículos seguros y conectados. *Estrategia de Seguridad Vial 2030*, cit., p. 213.

⁴⁷ <https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80295>

técnicos para autorizar su puesta en circulación; por otro lado, mediante el desarrollo de normas de circulación para estos vehículos; y, por último, respecto a la movilidad sostenible. Cuestiones que analizaremos a continuación y que una vez que se aprueben van a posibilitar que España sea uno de los países europeos que cuente con una regulación avanzada para vehículos automatizados.

4.2.1. Bases del marco regulatorio: Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial

En la medida en que la naturaleza de los vehículos autónomos trasciende la normativa actual, el legislador consideró oportuno, mediante la Ley 18/2021, de 20 de diciembre, en materia del permiso y licencia de conducción por puntos, introducir en la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobada por Real Decreto Legislativo 6/2015, de 30 de octubre, la base de un marco regulatorio sobre conducción y vehículos automatizados, con efectos de 21 de marzo de 2022. En su Exposición de Motivos recoge que el progreso tecnológico de la industria automotriz está permitiendo el desarrollo de dispositivos y vehículos equipados con diversas tecnologías, que vienen a proponer distintos niveles de automatización; y, en su grado máximo, la conducción plenamente automatizada o autónoma.

En sus artículos cuarto y quinto destaca, entre el listado de las competencias de regulación de esta materia, que será, siempre de conformidad con lo dispuesto en la ley, de la Administración General del Estado la regulación del vehículo automatizado; y del Ministerio del Interior las normas en materia de tráfico y seguridad vial que deberán cumplir los vehículos dotados de un sistema de conducción automatizado para su circulación, a excepción de los requisitos técnicos para la homologación de los vehículos cuyo desarrollo corresponde al Ministerio competente en materia de industria.

Se añade un nuevo artículo 11 bis relativo a las obligaciones del titular de un sistema de conducción automatizado de un vehículo, señalando que “deberá comunicar al Registro de Vehículos del organismo autónomo Jefatura Central de Tráfico las capacidades o funcionalidades del sistema de conducción automatizada, así como su dominio de diseño operativo, en el momento de la matriculación, y con posterioridad, siempre que se produzca cualquier actualización del sistema a lo largo de la vida útil del vehículo”. Por otro lado, en la disposición final segunda, se habilita normativa y específicamente al Gobierno para que regule el procedimiento por el que se certifique que un vehículo dotado de un sistema de conducción automatizado cumple con las normas de circulación; del mismo modo, también para que defina las capa-

ciudades de automatización y los entornos operacionales de uso, que se harán constar tanto en el Registro de Vehículos como en los permisos de circulación.

En cuanto a la información sobre las capacidades de conducción autónoma del vehículo se registrará en el permiso de circulación que se precisa para transitar. De esta manera, se establece que, en el caso de vehículos dotados de un sistema de conducción automatizada, se consignará en el permiso de circulación, conforme se desarrolle reglamentariamente, sus características, tanto de grado de automatización como del entorno operacional de uso (artículo 66.1).

4.2.2. Proyecto legislativo en materia de conducción automatizada: modificaciones del Reglamento General de Circulación y del Reglamento General de Vehículos

A raíz de esa competencia a la que anteriormente hacíamos referencia, el Ministerio del Interior ha impulsado un primer avance de la regulación de la circulación de vehículos autónomos, publicando el borrador del proyecto de Real Decreto en materia de conducción automatizada, que modificará el Reglamento General de Circulación, aprobado por Real Decreto 1428/2003, de 21 de noviembre y el Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, y que, en principio, está previsto que pueda aprobarse antes de que finalice el 2024⁴⁸. El objetivo de la propuesta es adaptar el Reglamento General de Vehículos a los requerimientos derivados de la normativa europea sobre homologación de vehículos totalmente automatizados, a fin de establecer los requisitos previos para su admisión en el tráfico, y también adaptar el Reglamento General de Circulación a los requisitos y funcionalidades de estos vehículos mediante el establecimiento de las condiciones de circulación genéricas y particulares que les puedan afectar.

La primera inferencia que podemos realizar es que la propuesta de regulación de la conducción automatizada en las carreteras españolas se va a llevar a cabo introduciendo modificaciones a la regulación existente, en lugar de apostar por el desarrollo de una regulación específica.

Por otro lado, se pretende aprovechar esta oportunidad para cumplir con la Estrategia de Seguridad Vial 2030, en el área estratégica vehículos seguros y

⁴⁸ https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/03_2024_Proyecto_RD_modifica_Reglamento_General_Circulacion_y_Reglamento_General_Vehiculos_conduccion_automatizada.pdf

conectados⁴⁹, para que nuestro país se convierta en laboratorio de pruebas del vehículo autónomo, impulsando un avance significativo en la regulación y las condiciones precisas tanto de los vehículos como de las vías para que sea posible implantar progresivamente una conducción automatizada segura⁵⁰. Así, una de las líneas de actuación clave dentro de este área, consiste en impulsar un despliegue seguro de los vehículos autónomos mediante acciones tales como el establecimiento de un marco regulatorio para todas las administraciones y entidades en el ámbito de la legislación sobre tráfico y seguridad vial.

También se acoge la necesidad de legislar para adaptar a nuestro ordenamiento el marco de la normativa europea que prevé una armonización tanto de la normativa de circulación como de los requisitos técnicos que se exijan a los vehículos como ha abordado la Comisión Europea al adoptar el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, introduciendo las nociones fundamentales y reglas básicas en lo que se refiere a los procesos y métodos para la homologación de los sistemas de conducción automatizados. En este sentido, el citado reglamento apuntaba, en sus considerandos, que en la medida en que los vehículos automatizados asumirán gradualmente las tareas del conductor, deben sus normas y requisitos técnicos, estar armonizados y adoptarse a escala de la Unión Europea, incluidos, en todo caso, los relativos

⁴⁹ <https://seguridadvial2030.dgt.es/areas-estrategicas/vehiculos-seguros-y-conectados/> En el punto 05.4 se fija como estrategia potenciar la conectividad e impulsar un despliegue seguro de los vehículos autónomos: “El objetivo de esta Línea de actuación es potenciar la contribución de la conectividad a una movilidad segura, mediante el desarrollo de nuevos casos de uso, sentar las bases normativas para el despliegue de la conducción automatizada y consolidar a España como laboratorio de pruebas del vehículo autónomo. En el ámbito de la conectividad, DGT 3.0 es, desde abril de 2017, la plataforma tecnológica con la que la Dirección General de Tráfico impulsa la conectividad entre vehículos y otros elementos móviles del tráfico, así como la distribución de datos a otras Administraciones y proveedores de servicios”. Por otro lado, resulta destacable el punto 05.8, en relación al aseguramiento de estos vehículos, ya que se pone de relieve que “la implantación de nuevos sistemas ADAS y la conectividad de los vehículos, que se espera cada vez mayor a corto y medio plazo, pueden proporcionar más y mejor información para implantar nuevos modelos de seguro relacionados con el comportamiento y las actitudes reales de los usuarios. También en este aspecto se debe considerar a los nuevos tipos de vehículos, que se están incorporando igualmente a la movilidad conectada”.

⁵⁰ Para la autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general, se cuenta con la Instrucción VEH 2022/07, cuyo objetivo es la regulación de la concesión de las autorizaciones especiales para la realización de pruebas y ensayos de investigación con vehículos automatizados en vías abiertas al tráfico en general. DGT (2024). Vehículos seguros y conectados. *Estrategia de Seguridad Vial 2030*, cit., p. 7.

a garantías de seguridad verificables para la toma de decisiones por parte de vehículos automatizados. Conforme a la disposición de desarrollo incorporada al artículo 11, la Comisión adoptó el 5 de agosto de 2022 el Reglamento de Ejecución (UE) 2022/1426 por el que se establecen normas en cuanto a los procedimientos uniformes y las especificaciones técnicas para la homologación de tipo del sistema de conducción automatizada (ADS). A tal efecto, el proyecto legislativo establece como requisito general que los sistemas de conducción automatizada deberán contar con el correspondiente certificado de homologación emitido según las condiciones contempladas en dicho Reglamento (UE) 2019/2144, y en particular, en el Reglamento de Ejecución (UE) 2022/1426, al que nos hemos referido. Ahora bien, sin perjuicio de lo allí dispuesto, deberán ser capaces por sí mismos de:

1. Dominar de forma independiente y segura la tarea de conducción dinámica dentro de un entorno operacional de uso definido, sin que ninguna persona intervenga en los controles o supervise la operación.
2. Cumplir las normas de circulación, así como disponer de un sistema de prevención de accidentes.
3. Únicamente debe operar dentro de su dominio de diseño operativo definido, sin posibilidad de ser activado fuera de aquél.
4. Llevar el vehículo a motor de forma independiente a un estado de riesgo mínimo si las condiciones de circulación y de seguridad vial lo requieren.
5. Reconocer los límites del sistema y poner el vehículo en un estado de riesgo mínimo de forma autónoma cuando se alcance un límite del sistema, cuando ocurra un fallo técnico o accidente, o cuando se alcancen los límites del dominio de diseño operativo definido, priorizando siempre la seguridad vial y la fluidez del tráfico.
6. Poder ser desactivado en cualquier momento por un operador autorizado.
7. En caso de desactivación, el sistema deberá asegurar que el operador puede tomar el control de forma segura y efectiva. En su defecto, deberá llevar el vehículo de forma independiente al estado de riesgo mínimo.

Además, el proyecto establece otros tres requisitos precisos para obtener un permiso de circulación para un vehículo dotado de un sistema de conducción automatizada, en el caso de que sus funcionalidades permitan la operación del vehículo por medio de un operador de intervención a distancia. Para ello, se exige que el sistema de conducción automatizada deba, adicionalmente:

1. Comprobar la maniobra de conducción especificada por el operador remoto, si existiere, y no llevarla a cabo en el caso de esta ponga en peligro

a los usuarios que participan en la circulación o a los transeúntes, debiendo priorizar llevar el vehículo de forma independiente a un estado de riesgo mínimo.

2. Informar inmediatamente cualquier deterioro de su funcionalidad al operador remoto, si existiere.

3. Indicar al operador remoto, si existiera conforme a sus condiciones de uso, la necesidad de activar una maniobra de conducción alternativa sobre el vehículo, la desactivación del sistema con suficiente tiempo de respuesta, o la activación de las señales necesarias.

Por lo tanto, el legislador insta a reconocer los límites del sistema y a poner el vehículo en un estado de riesgo mínimo cuando se ponga en peligro a otros usuarios y peatones. También el sistema debe poder ser desactivado en cualquier momento por un operador autorizado y asegurar que el operador puede tomar el control de forma segura y efectiva; y en su defecto, deberá llevar el vehículo de forma independiente al estado de riesgo mínimo. De este modo, el legislador pretende ser coherente con el Reglamento europeo de IA.

La propuesta añade un nuevo artículo 14 bis (Sistemas de conducción automatizada) al Reglamento General de Vehículos (RGV) que dispone que los vehículos dotados de sistemas de conducción automatizada no pueden circular si no cuentan con su correspondiente permiso de circulación expedido por la Jefatura Central de Tráfico, que especificará las funcionalidades y dominio de diseño operativo conforme a los requisitos contemplados en el anexo XIX de este reglamento, destinado a asegurar su aptitud para circular con seguridad. Y, por otro lado, se añade también al RGV la obligación de los titulares del sistema de conducción automatizada de comunicar en un plazo de 48 horas la variación de las funcionalidades del sistema (artículo 30.2). El legislador tiene en cuenta, de este modo, la posibilidad de actualización online de los sistemas de los vehículos que pueden modificar sus funciones para que sean comunicadas en un breve lapso de tiempo.

En dicho anexo XIX, además de esa sección relativa a los requisitos generales, se incorpora una sección 1ª de definiciones. Se trata de un conjunto muy amplio de 36 nuevas definiciones⁵¹, entre las que destacan:

⁵¹ Las definiciones del nuevo Anexo XIX “Sistemas de Conducción Automatizada” son las siguientes: «Vehículo totalmente automatizado», «sistema de conducción automatizada» (ADS), «dominio del diseño operativo» (ODD), «Tareas dinámicas de la conducción (DDT)», «Registrador de datos de incidencias», «característica del ADS», «función del ADS», «funciones operativas», «funciones tácticas» de la tarea de conducción dinámica, «defecto», «fallo», «vigilancia en servicio», «información en servicio», «vida útil del ADS», «ciclo de vida del ADS», «mal funcionamiento», «maniobra de riesgo mínimo», «condición de riesgo mínimo», «detección y respuesta de objetos y eventos» («OEDR»), «escenario», «escenarios de tráfico nominales», «escenarios críticos», «escenarios de fallo», «funcionamiento de emergencia», «operador a bordo», «operador de interven-

«Vehículo totalmente automatizado»: *Vehículo de motor diseñado y construido para desplazarse de manera autónoma sin supervisión por parte del conductor.*

«Sistema de conducción automatizada» (ADS): *el hardware y el software que son capaces colectivamente de realizar la totalidad de la tarea de conducción dinámica de forma continuada en un ámbito de diseño operativo específico.*

«Dominio del diseño operativo» (ODD): *las condiciones de funcionamiento en las que está diseñado específicamente para funcionar un ADS determinado, incluidas, entre otras, las restricciones medioambientales, geográficas y de la hora del día, o el requisito de presencia o ausencia de determinadas características del tráfico o de la vía pública.*

«Tareas dinámicas de la conducción» (DDT): *todas las funciones operativas en tiempo real y funciones tácticas necesarias para el funcionamiento del vehículo, excluidas funciones estratégicas como la programación del trayecto y la selección de destinos y puntos de ruta, incluidas, entre otras, las siguientes subáreas: (a) control del movimiento lateral del vehículo mediante la dirección (operativa); (b) control del movimiento longitudinal del vehículo mediante aceleración y desaceleración (operativa); (c) seguimiento del entorno de conducción a través de la detección, reconocimiento y clasificación de objetos y eventos y la preparación de la respuesta (operativa y táctica); (d) ejecución de la respuesta a objetos y eventos (operativa y táctica); (e) planificación de la maniobra (táctica); (f) mejora de la visibilidad mediante iluminación, bocina, señales, indicaciones, etc. (táctica).*

«Defecto»: *una situación anormal que puede causar un fallo. Puede afectar al hardware o al software.*

«Fallo»: *el cese de un comportamiento previsto de un componente o sistema del ADS debido a la aparición de un defecto.*

«Operador a bordo»: *persona situada dentro del vehículo totalmente automatizado que, cuando corresponda al concepto de seguridad ADS, podrá: a) activar, reinicializar, o desactivar el ADS; b) solicitar al ADS que inicie una maniobra de riesgo mínimo; c) confirmar una maniobra propuesta por el ADS; «Operador a bordo»: mientras el vehículo está parado; d) después de una maniobra de riesgo mínimo, mientras el vehículo totalmente automatizado está parado, solicitar al ADS que realice con seguridad una maniobra de baja velocidad limitada a 6 km/h con el rendimiento restante para evacuar el vehículo totalmente automatizado a una ubicación preferible cercana; e) seleccionar o modificar la planificación de un itinerario o puntos de parada para los usuarios, o f) prestar asistencia a los pasajeros del vehículo totalmente automatizado en situaciones debidamente identificadas.*

ción a distancia (operador remoto)», «capacidades a distancia», capacidades diseñadas específicamente para apoyar la intervención a distancia; «número de identificación de software R2022/1426 (R2022/1426SWIN)», «riesgo excesivo», «seguridad funcional», «seguridad operativa», «estrategia de control», «tiempo de colisión», «tipo de vehículo con respecto al ADS», y «vehículos de modo dual». Nos remitimos a la propuesta normativa, que recoge dichas definiciones.

«Operador de intervención a distancia (operador remoto)»: : *cuando corresponda al concepto de seguridad ADS, la persona o personas situadas fuera del vehículo totalmente automatizado que puedan desempeñar a distancia las tareas del operador a bordo, siempre que sea seguro hacerlo.*

En el Reglamento General de Circulación (RGC) se incorpora en el artículos 3 bis y 18 bis la definición de vehículos totalmente automatizados, que serán aquellos “dotados de un sistema de conducción automatizada, diseñados y contruidos para desplazarse de manera autónoma sin supervisión por parte del conductor”. El que expresamente se recoja esta ausencia de supervisión del conductor implica que ya sí que nos encontraríamos vehículos con conducción autónoma de nivel 4 y nivel 5, ya que en los otros niveles se precisa el control del conductor. Por otro lado, se dispone que este sistema solo podrá ser activado y funcionar “dentro de su entorno operacional y conforme a sus condiciones de uso, debiendo cumplir las normas de circulación de vehículos previstas en este reglamento y en su normativa de desarrollo”. Por lo tanto, solo puede utilizarse en dicho entorno y bajo determinadas condiciones de uso, siendo en tal caso el sistema de conducción el que sea considerado como el conductor del vehículo, debiendo los ocupantes adaptar su comportamiento de acuerdo con las condiciones de uso de tal sistema y a la normativa reglamentaria.

Por su parte, el nuevo artículo 18 bis del RGC establece las obligaciones tanto relativas al comportamiento del vehículo en el tráfico como a las propias del titular del sistema de conducción autónoma en lo referente a la operación de los vehículos, añadiéndose un nuevo anexo V sobre normas y condiciones particulares de circulación cuando la conducción se produzca de manera automatizada⁵², que se compone de dos secciones. Una relativa a las condiciones generales de circulación que deben satisfacer los vehículos totalmente auto-

⁵² El Anexo V establece las normas y condiciones particulares de circulación de los vehículos dotados de un sistema de conducción automatizada, estableciendo las siguientes condiciones generales de circulación “1. El vehículo a motor dotado de un sistema de conducción automatizada debe cumplir con los requisitos técnicos establecidos en la normativa aplicación y en el Reglamento General de Vehículos, así como lo dispuesto en la sección 2ª de este anexo. 2. El uso de estos vehículos deberá estar amparado por la autorización administrativa contemplada en el artículo 14bis del Reglamento General de Vehículos y en las condiciones prescritas en sus anexos XIII y XIX. 3. Su circulación se ajustará a las normas generales de este reglamento que les sean de aplicación. En todo caso prevalecerán las condiciones de circulación particulares que se fijen en la sección 2ª de este anexo. 4. El vehículo a motor dotado de un sistema de conducción automatizada sólo podrá ser activado y utilizado en un entorno operacional de uso definido, que deberá ser previamente comunicado por el titular del sistema conforme a los requisitos del Reglamento General de Vehículos, y cumpliendo las normas de este reglamento. 5. En todo momento se observarán las disposiciones restrictivas de tránsito especialmente establecidas, las que se hallen señalizadas en la vía o las que sean indicadas por la autoridad encargada de la regulación y control del tráfico. 6. La circulación deberá suspenderse saliendo previamente de la plataforma de circulación siempre que el sistema detecte que no puede continuar operando dentro de su entorno operacional de uso o sufra una avería o accidente

matizados, y la segunda que dispone la creación de un Manual de Circulación Segura, en el que se establecerán, como su propio nombre indica, las condiciones para la circulación segura de estos vehículos en las vías públicas.

En el borrador también se prevé que la Jefatura Central de Tráfico redacte, en un plazo máximo de 24 meses, un Manual de de Certificación de los sistemas de conducción automatizada, en el que se establezcan las condiciones y los requisitos particulares de aceptación y admisión de procedimientos de autocertificación por el propio titular del sistema; además del Manual de Circulación Segura para los vehículos autónomos. Si se cumplen los requisitos contemplados en el Reglamento y el anexo, así como en el Manual de Certificación, la autoridad responsable emitirá, a petición del titular del sistema, un permiso de circulación para el vehículo dotado de un sistema de conducción automatizada.

4.2.3. Proyecto de Ley de Movilidad Sostenible

El capítulo segundo del Proyecto de Ley de Movilidad Sostenible⁵³, artículos 82 y siguientes, regula el vehículo automatizado, donde se incluyen principios de actuación de las administraciones públicas para la regulación y promoción de la introducción progresiva de los vehículos automatizados en el sistema de transportes. Para los fines de este trabajo, podemos destacar el de la seguridad tanto física como frente a la ciberseguridad, la sostenibilidad o la protección de datos, entre otros⁵⁴.

Respecto a los vehículos automatizados en el sistema de transportes y movilidad por carretera, recoge esa necesidad de adecuar las habilitaciones de uso, señalando que “los órganos competentes para la regulación de las auto-

que impida continuar su marcha, excepto cuando un operador, remoto o presencial, pueda tomar el control del vehículo de forma segura y continuar su marcha, en las condiciones que se establezcan”.

⁵³ Proyecto de Ley de Movilidad Sostenible, publicado en el BOCG, 23 febrero de 2024. Disponible en https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-9-1. PDFTimes New Roman

⁵⁴ El artículo 82 del Proyecto de Ley de Movilidad Sostenible destaca la seguridad física de la movilidad y seguridad frente a ataques a través de sistemas informáticos y ciberseguridad; la sostenibilidad ambiental y eficiencia del sistema de transportes; buena regulación, aprovechando la experiencia acumulada para su mejora continua, así como la de los procedimientos de gestión y mantenimiento de las infraestructuras digital y física; la protección de los derechos de las personas en el desarrollo de esta tecnología y de los datos, para asegurar que sea inclusiva, accesible, y no discriminatoria por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social; fomento de la colaboración público-privada en la regulación y el diseño del despliegue de esta tecnología, y atendiendo, siempre, a las necesidades de movilidad de los ciudadanos y ciudadanas; y coordinación entre administraciones para la operabilidad del vehículo automatizado entre las diferentes redes de infraestructura.

rizaciones habilitantes para la realización de transporte de personas o mercancías por carretera adecuarán, en su caso, los requisitos y condiciones para habilitar el uso de vehículos automatizados en el transporte” (artículo 85 del Proyecto).

5. REGULACIÓN DE LOS SISTEMAS DE ALTO RIESGO EN LA INTELIGENCIA ARTIFICIAL

Los algoritmos de *machine y deep learning* de la IA, a través de la tecnología a la que nos venimos refiriendo, permite al vehículo analizar la conducción, predecir los movimientos de otros usuarios, anticipar riesgos y planificar la trayectorias más segura del vehículo, es por ello, que es preciso analizar la regulación que sobre IA se está llevando a cabo en el ámbito europeo bajo tres ejes, el reglamento europeo de IA y las propuestas de directivas sobre productos defectuosos y la de responsabilidad en materia de IA.

5.1. REGLAMENTO EUROPEO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL

En el Libro Blanco sobre la inteligencia artificial, publicado en Bruselas el 19 de febrero de 2020, se definen las opciones existentes para promover la adopción de la IA y abordar los riesgos vinculados a determinados usos de esta nueva tecnología, instando a revisar la legislación vigente de la UE para determinar si contempla adecuadamente los riesgos y oportunidades, así como los requisitos de las aplicaciones de IA, si pueden aplicarse de manera efectiva y si se requieren ajustes o una nueva legislación⁵⁵. Dando un paso más, se aprobó una propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (la llamada Ley de Inteligencia Artificial, LIA), teniendo por objeto inspirar confianza en los ciudadanos, usuarios y empresas, proporcionando para ello un marco jurídico basado en el riesgo e imponiendo una serie de obligaciones a los distintos agentes, destinado a lograr que la IA sea un instrumento fiable y seguro para las personas y una fuerza positiva en la sociedad, que incremente el bienestar humano⁵⁶. Esta propuesta ha tardado más

⁵⁵ Comisión Europea, Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final.

⁵⁶ Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, COM/2021/206 final.

de tres años en aprobarse, con modificaciones, lo que ha tenido lugar mediante el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial, RIA)⁵⁷. Y ello en coordinación con el Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, cuya propuesta inicial fue aprobada en la misma fecha, y que velará para que la nueva generación de maquinaria garantice la seguridad de los usuarios y consumidores⁵⁸. También debe tenerse en cuenta que, aunque el RIA entró en vigor el 1 de agosto, existe un cronograma de implementación gradual⁵⁹, que si bien proporciona tiempo para la adaptación, también puede crear incertidumbres regulatorias temporales. La Oficina Europea de IA, creada en febrero de 2024, en el seno de la Comisión, será la que supervise el cumplimiento y la aplicación del RIA con los Estados miembros⁶⁰.

Respecto al objeto de este Reglamento, debemos delimitar, en primer lugar, su ámbito de aplicación objetivo, realizando una mención a lo que se considera sistema de IA, definición que ha sido tomada de la “Recomendación del Consejo de la OCDE sobre Inteligencia Artificial”⁶¹ (que fue modificada en noviembre de 2023 para proporcionar una definición más apropiada; y

⁵⁷ Publicado en el DOUE, núm. 1689, de 12 de julio de 2024. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079>

⁵⁸ No obstante, no resulta de aplicación a los vehículos a motor, tal y como dispone el artículo 2.2. g) que excluye de su ámbito “los vehículos de motor y sus remolques, así como los sistemas, componentes, unidades técnicas independientes, piezas y equipos diseñados y fabricados para dichos vehículos, homologados que se incluyen en el ámbito de aplicación del Reglamento (UE) 2018/858, excepto las máquinas montadas en esa clase vehículos;”.

⁵⁹ El RIA será plenamente aplicable 24 meses después, excepto en lo relativo a las prohibiciones de prácticas prohibidas (6 meses después) códigos de práctica (9 meses después), las normas de uso general, incluida la gobernanza (12 meses después) y las obligaciones para sistemas de alto riesgo (36 meses). Tesone, R. (2024), El Reglamento de Inteligencia Artificial de la Unión Europea: “Un Reglamento para una Nueva Era”. Principales Aspectos y Obligaciones, *El derecho.com*, Lefebvre. 12 julio 2024. <https://elderecho.com/el-reglamento-de-inteligencia-artificial-de-union-europea-principales-aspectos-y-obligaciones>; y Vestri G. (2024): “La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA)”, *Diario La Ley*, n.º 10550.

⁶⁰ European AI Office. <https://digital-strategy.ec.europa.eu/en/policies/ai-office>

⁶¹ Dicha Recomendación del Consejo de la OCDE sobre Inteligencia Artificial es un conjunto de directrices y principios para el desarrollo y despliegue de sistemas de IA, si bien no son vinculantes y carecen de un mecanismo formal de aplicación, si bien son acogidos, entre otros, por el G20, la UE, Japón, Estados Unidos, y tenido en cuenta por Naciones Unidas. Fue adoptada por el Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en mayo de 2019 e incluye cinco principios clave para la gobernanza de la IA.

que ha sido actualizada recientemente, el 3 de mayo de 2024, tras la aprobación del Reglamento de IA, actualizando sus principios sobre la IA). El artículo 3 define «sistema de IA» en los siguientes términos: “un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales”⁶².

Es importante advertir que la propuesta de regulación de este primer marco normativo no se ocupa de la responsabilidad civil ya que no contiene disposiciones sobre los daños causados por los sistemas de IA. Se parte de la división de los sistemas de IA, que había establecido la propuesta de la LIA conforme a cuatro niveles de riesgo (que imponía una serie de obligaciones específicas solo a los de riesgo alto y riesgo limitado ya que la primera categoría, la de riesgo inadmisible, la prohibía, y la de riesgo nulo quedaba fuera de su ámbito de aplicación). El RIA establece, entre sus aspectos más relevantes, las prácticas prohibidas de IA, que no son aceptables (artículo 5) y se centra en los sistemas de IA de alto riesgo, estableciendo una clasificación de estos sistemas de alto riesgo (artículo 6 y Anexo III), define los requisitos que deben cumplir (artículos 8 a 15) y las obligaciones aplicables a los operadores pertinentes (artículos 16 y siguientes), así como impone obligaciones de transparencia a determinados sistemas de IA (artículo 50). Además, el Reglamento se entiende sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos (artículo 2.9). De este modo, se establece un enfoque basado en el riesgo (*risk-based approach*), estableciendo una regulación para los sistemas de alto riesgo, normas armonizadas para el desarrollo, la introducción en el mercado y la utilización de estos sistemas, imponiendo obligaciones con el fin de promover la adopción de una inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE, y proteger frente a los efectos

⁶² La traducción de la Recomendación efectuada por la OECD sobre sistema de IA, y que ha adoptado el RIA, resulta más clara: “Sistema de IA: Un sistema de IA es un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, cómo generar información de salida como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos reales o virtuales. Una vez implementados, los distintos sistemas de IA presentan diversos niveles de autonomía y varían en su capacidad de adaptación”. <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#translations>

perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación.

Respecto a la consideración de los sistemas de IA de los vehículo autónomos como de alto riesgo, en el Anexo III se contempla un listado, donde se incluyen los sistemas de IA que formen parte de infraestructuras críticas, recogiendo expresamente, entre otras, los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas y del tráfico rodado. Ahora bien, es posible que, aunque el sistema se encuentre en ese listado, tras su evaluación no se considere como tal por el uso específico que se le vaya a dar⁶³. Por otro lado, tienen también esa consideración, a los efectos de aplicación del Reglamento, los productos regulados por los actos legislativos de armonización de la Unión enumerados en la sección B del anexo I, donde se incluye el Reglamento (UE) 2019/2144 (artículo 2.2). Y, además, el artículo 6 considera que también son sistemas de IA de alto riesgo cuando se reúnan las dos condiciones que se indican a continuación: (a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y (b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I⁶⁴.

Los sistemas de IA de alto riesgo van a estar sujetos a una serie de requisitos: sistema de gestión de riesgos; datos y gobernanza de datos; documentación técnica; conservación de registros; transparencia y comunicación de información a los responsables del despliegue; supervisión humana; precisión, solidez y ciber-

⁶³ “La clasificación del nivel de riesgo del sistema de IA dependerá del contexto de su uso específico de acuerdo con los criterios establecidos en el art. 6.3 y los elementos interpretativos expuestos en los Considerandos 52 y 53 del RIA. Aquellos proveedores que consideren que su sistema de IA no constituye un alto riesgo, a pesar de que su uso se enmarque en alguna de las áreas de Anexo III, deberán realizar y documentar una evaluación antes de que el sistema de IA sea introducido en el mercado o se puesto en servicio (art. 6.4)”. Eguiluz Castañeira, J. y Fernández Hernández, C., “Diez puntos críticos del Reglamento europeo de Inteligencia Artificial”, *La Ley*, 21 mayo 2024. <https://diariolaley.laleynext.es/dll/2024/06/28/diez-puntos-criticos-del-reglamento-europeo-de-inteligencia-artificial>

⁶⁴ Si bien, dispone el artículo 2.2. que a los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en dicha sección B del anexo I, solo se les va a aplicar el artículo 6, apartado 1, y los artículos 102 a 109 y el artículo 112; y artículo 57 en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión.

seguridad (artículos 8 a 15); y también a unas obligaciones estrictas de sus proveedores (artículos 16 a 22), al mismo tiempo que también se impondrán otras o a los importadores (artículo 23), distribuidores (artículo 24) y responsables del despliegue de sistemas de IA de alto riesgo (artículo 26).

Entre estos requisitos, destacamos la necesidad de una vigilancia humana, que puede resultar un elemento decisivo, de manera que “puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas” (artículo 14). Si bien, hay que precisar, como señala la RIA, en su considerando 27, de conformidad con las directrices del Grupo independiente de expertos de alto nivel sobre IA, por «acción y supervisión humanas» se entiende que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por seres humanos. De este modo, se establecen unas medidas de supervisión, que deben ser proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo, y que deben garantizarse mediante una, o ambas, de las siguientes medidas: (a) *las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio*; b) *las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue* (artículo 14.3)⁶⁵.

El reglamento introduce, por otro lado, modificaciones en varias regulaciones y directivas de la UE en diversos sectores afectados por la IA para alinearlas con el nuevo marco normativo, garantizando su coherencia a este entorno. Entre las modificaciones claves se incluye la del Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, relativo a los requisitos de

⁶⁵ A tales efectos, las personas físicas a quienes se encomiende la supervisión humana podrán, según proceda y de manera proporcionada: “(a) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados; (b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión; (c) interpretar correctamente los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles; (d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere; (e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura” (artículo 14.4).

homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública. De hecho, en el Considerando 49 del RIA se indica que, en relación con los sistemas de IA de alto riesgo que son componentes de seguridad de productos o sistemas, o que son en sí mismos productos o sistemas que entran en el ámbito de aplicación de diversas normas de la UE, donde se incluye el Reglamento (UE) 2019/2144 “procede modificar dichos actos para garantizar que, cuando la Comisión adopte actos delegados o de ejecución pertinentes basados en ellos, tenga en cuenta los requisitos obligatorios para los sistemas de IA de alto riesgo previstos en el presente Reglamento, atendiendo a las particularidades técnicas y reglamentarias de los distintos sectores y sin interferir con los mecanismos y las autoridades de gobernanza, evaluación de la conformidad y control del cumplimiento vigentes establecidos en dichos actos”. En virtud de lo expuesto, el artículo 109 del RIA modifica el artículo 11 del Reglamento (UE) 2019/2144, añadiendo un tercer párrafo en los siguientes términos: “Al adoptar actos de ejecución en virtud del apartado 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento, es decir, los requisitos de los sistemas de IA de alto riesgo previstos en el artículo 8 (Cumplimiento de los requisitos), artículo 9 (Sistema de gestión de riesgos), artículo 10 (Datos y gobernanza de datos), artículo 11 (Documentación técnica), artículo 12, (Conservación de registros), artículo 13 (Transparencia y comunicación de información a los responsables del despliegue), artículo 14 (Supervisión humana), artículo 15 (Precisión, solidez y ciberseguridad). Por lo tanto, habrá que tener en cuenta dichos requisitos esenciales cuando se apruebe la legislación delegada o de ejecución.

5.2. DIRECTIVA SOBRE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS

Tras la propuesta de Reglamento europeo, por el que se establecían normas armonizadas en materia de IA (LIA, 2021), sobre la necesidad de regular estos sistemas de IA en función del riesgo generado a los ciudadanos, se consideró que era precisa una actualización de la Directiva por productos defectuosos para responder de los daños causados por estos productos dotados de

sistemas de IA⁶⁶. Ahora bien, téngase en cuenta que esta normativa opera para todos los ámbitos y no solo para la IA, y además requiere de la existencia de un defecto⁶⁷. Por ello, al delimitar la responsabilidad por los daños causados por los sistemas de IA debemos establecer el ámbito de actuación en el que nos encontramos y la legislación especial que pudiera ser aplicable.

La Comisión Europea ha impulsando una reforma para adaptarla a los enormes cambios ocasionados por la digitalización a través de Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, existiendo ya una Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, que lo ha aprobado en primera lectura, que ahora pasará a ser revisada por el Consejo⁶⁸. Con la revisión de la Directiva, se pretende crear unas condiciones de competencia más equitativas entre los fabricantes de la UE y de terceros países para que cuando las personas consumidoras resulten perjudicadas por productos inseguros importados de fuera de la UE puedan dirigirse al importador o al representante de la UE del fabricante para obtener una indemnización⁶⁹.

⁶⁶ Hasta ahora, el marco legal europeo de referencia en materia de responsabilidad por producto defectuoso había venido siendo la Directiva 85/374/CEE de 25 de julio de 1985, que fue traspuesta en nuestro país por la Ley 22/1994, de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos y, posteriormente, siendo integrada en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

⁶⁷ “La Propuesta de Directiva sobre DRPD tiene un ámbito de aplicación distinto a la dictada sobre responsabilidad civil e inteligencia artificial por cuanto se refiere a cualesquiera tipos de productos, y no sólo a aquéllos dotados de inteligencia artificial, aunque, también a diferencia de aquella, exige que aquéllos adolezcan de un defecto”. Atienza Navarro (2023), ¿Una nueva responsabilidad por productos defectuosos?, op. cit., p. 5.

⁶⁸ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. COM/2022/495 final. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0495>. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos (COM(2022)0495 - C9-0322/2022 -2022/0302(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.pdf. La versión oficial de este texto de la Directiva se encuentra disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.html.

⁶⁹ Para un análisis de las soluciones adoptadas en la propuesta, véanse Rodríguez de las Heras Balcells T. (2023). La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial. *La Ley mercantil*, n.º 103; y Atienza Navarro, M. L. (2023). ¿Una nueva responsabilidad por productos defectuosos?. Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)”. *InDret*, n.º 2, pp. 1-53. <https://doi.org/10.31009/InDret.2023.i2.01>; Gómez Ligüerre, C. (2022). La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos. *InDret*, n.º 4, 2022. <https://indret.com/la-propuesta-de-directiva-sobre-responsabilidad-por-danos-causados-por-productos-defectuosos/>

Por un lado, se extiende la definición de «producto» a “cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble”, así como también se incluyen expresamente a los archivos de fabricación digital y los programas informáticos (artículo 4). También se exige a los fabricantes un mayor acceso a la prueba (artículo 9), se reduce la carga de la prueba para las víctimas en casos complejos (artículo 10), se otorga más flexibilidad en las restricciones temporales para presentar reclamaciones, y se añaden factores como la interconexión o las funciones de autoaprendizaje de los productos a la lista de factores que deben tener en cuenta a la hora de evaluar el carácter defectuoso⁷⁰. Y, del mismo modo, se tiene en cuenta las actualizaciones del producto a través de programas informáticos, o por el aprendizaje continuo de un sistema de IA, a la hora de considerar su puesta en servicio⁷¹.

Por otro lado, respecto a la imputación de la responsabilidad, se sustituye la referencia al productor, por la de «operadores económicos responsables de los productos defectuosos», para dar cabida al fabricante, al importador, al representante autorizado, al distribuidor, y que el consumidor siempre pueda dirigirse para *reclamar una indemnización al importador del producto y al representante autorizado del fabricante (artículo 37)*.

La novedad más importante que se ha introducido en la última versión ha sido respecto de la exoneración de la responsabilidad por los riesgos del desarrollo, permitiendo ahora que los Estados miembros puedan establecer

⁷⁰ De este modo, señala el Considerando (32) : “Con el fin de reflejar la creciente prevalencia de productos interconectados, la evaluación de la seguridad de un producto también debe tener en cuenta los efectos razonablemente previsibles de otros productos en el producto en cuestión, como por ejemplo en un sistema doméstico inteligente. También debe tenerse en cuenta el efecto sobre la seguridad de un producto de su capacidad de aprendizaje o de adquisición de nuevas características tras su introducción en el mercado o su puesta en servicio, a fin de reflejar la expectativa legítima de que el programa informático de un producto y los algoritmos subyacentes estén diseñados de manera que se evite un comportamiento peligroso del producto. Por consiguiente, un fabricante que diseñe un producto con la capacidad de desarrollar un comportamiento inesperado debe seguir siendo responsable de todo comportamiento que cause daños. Para reflejar el hecho de que, en la era digital, muchos productos permanecen bajo el control del fabricante tras su introducción en el mercado, el momento en que un producto deja de estar bajo el control del fabricante también debe tenerse en cuenta en la evaluación de su seguridad. Un producto también puede considerarse defectuoso debido a su vulnerabilidad en materia de ciberseguridad, por ejemplo cuando el producto no cumpla los requisitos de ciberseguridad relevantes para la seguridad.

⁷¹ Considerando (40) “Dado que los productos pueden diseñarse de manera que permitan introducir modificaciones a través de cambios en los programas informáticos, incluidas mejoras de estos, deben aplicarse a las modificaciones introducidas mediante una actualización o mejora de los programas los mismos principios que se aplican a las modificaciones realizadas de otras maneras. Cuando una modificación sustancial se realice a través de una actualización o mejora de un programa informático, o por el aprendizaje continuo de un sistema de IA, debe considerarse que el producto sustancialmente modificado se comercializa o pone en servicio en el momento en que se introduzca realmente la modificación”.

limitaciones a esta causa de exoneración en determinados tipos de productos (artículo 18), resultando en el caso de los vehículos autónomos aconsejable excluir dicha posibilidad de alegación sobre el defecto para generar confianza sobre la cobertura de los daños⁷².

Tal y como se encuentra configurado este sistema, considero que resulta de difícil aplicación para que las víctimas puedan reclamar daños directamente a los operadores económicos como el fabricante, siendo una vía más sencilla y directa la que proporciona el procedimiento de reclamación de daños de la LRCSCVM, que otorga mayores garantías de que la víctima sea indemnizada, y sin perjuicio de que la aseguradora del vehículo pueda reclamar contra el fabricante por los defectos del mismo. Téngase en cuenta, además, que en el sistema recogido en esta ley el defecto del vehículo no se considera un supuesto de fuerza mayor extraña a la conducción para exonerar de responsabilidad en el caso de daños a las personas, como tampoco la rotura o fallo de alguna de sus piezas o mecanismos (artículo 1.1 LRCSCVM).

5.3. PROPUESTA DE DIRECTIVA RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL A LA INTELIGENCIA ARTIFICIAL

Tal y como puso de relieve el Informe de la Comisión europea sobre las repercusiones en materia de seguridad y responsabilidad civil de la IA, internet de las cosas y robótica, de 19 de febrero de 2020, la existencia de un marco claro en materia de seguridad y responsabilidad civil es particularmente importante cuando surgen estas nuevas tecnologías para así garantizar tanto la protección de los consumidores como la seguridad jurídica para las empresas⁷³. Aunque se considera que, en principio, la normativa europea y las nacionales en materia de responsabilidad civil pueden hacer frente a las vicisitudes jurídicas derivadas de las tecnologías emergentes, la dimensión y el efecto combinado de las dificultades que plantea la IA podrían dificultar la indemnización de las víctimas. Por lo tanto, el reparto de los costes cuando se produce un daño puede ser injusto o ineficiente con arreglo a las normas actuales.

⁷² Navarro-Michel, M. (2020). Vehículos automatizados y responsabilidad por producto. *Revista de Derecho Civil*, vol. VII, nº 5, p. 215.

⁷³ Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, COM/2020/64 final. Disponible en [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)64&lang=es](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)64&lang=es)

Además, se ponía de manifiesto las dificultades probatorias sobre la causalística del daño derivado de la IA y la necesidad de un mismo nivel de protección a las víctimas de daños causados por otros productos; junto con el Libro Blanco sobre la IA (2020), que marcaba el objetivo de promover la adopción de la IA abordando los riesgos vinculados a su uso, que determinaba que para considerar a las aplicaciones de IA de riesgo elevado había que tener en cuenta el sector donde se utilizan, y los riesgos a la seguridad, los derechos de los consumidores y los derechos fundamentales⁷⁴.

La búsqueda de un marco legal que dotara de seguridad jurídica a la IA, que promoviera la innovación, garantizara la seguridad y protegiera los derechos humanos, originó la aprobación de la Resolución del Parlamento Europeo de 20 de octubre de 2020⁷⁵ con unas recomendaciones destinadas a la Comisión con el objeto de establecer unas bases para establecer el régimen de responsabilidad civil aplicable en el futuro, instaurando un sistema del que deban responder quienes causan un daño trabajando con una IA de riesgo. Y, del mismo modo, además, la Resolución del Parlamento Europeo sobre la inteligencia artificial en la era digital (2022) aseguraba que la IA no siempre debe de estar regulada en tanto que tecnología, sino que su regulación debe ser proporcional al tipo de riesgo individual o social que entraña el uso de un sistema de IA; incidiendo también en la importancia de distinguir entre casos de uso de la IA de «alto riesgo», que requiere más salvaguardias legislativas estrictas, y de «bajo riesgo», que en muchos casos requerirá requisitos de transparencia para los usuarios finales y los consumidores⁷⁶.

⁷⁴ Comisión Europea, Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final.

⁷⁵ Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html. La propuesta incorpora, por un lado, un Reglamento sobre principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial y, por otro lado, una propuesta de Reglamento relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial.

⁷⁶ La Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital, en su punto 19, incide en que el nivel de riesgo de una determinada aplicación de IA varía en función de la probabilidad de que se produzcan daños y su gravedad, por lo que considera que “los requisitos legales deben ajustarse a ello, en consonancia con un enfoque basado en el riesgo y teniendo debidamente en cuenta, cuando esté justificado, el principio de precaución; destaca que en las situaciones presentes o futuras en las que, para un uso en concreto, los sistemas de IA planteen riesgos elevados para los derechos fundamentales y humanos, se requiere una supervisión totalmente humana y una intervención reguladora, y que, habida cuenta de la velocidad del desarrollo tecnológico, la regulación de los sistemas de IA de alto riesgo debe ser flexible y estar orientada al futuro”.

La Propuesta de Reglamento relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial⁷⁷, incorporada a la Resolución del Parlamento, indicaba que no se pretendía sustituir los regímenes de responsabilidad civil existentes (incluso se indicaba, quizás, con cierto optimismo, que estos operan correctamente), sino efectuar ajustes para que puedan aplicarse a este escenario. Además, se perseguía que los operadores de las tecnologías dotadas de IA que presentaran un riesgo elevado contasen con un seguro obligatorio, tal y como acontece con los vehículos de motor. Su ámbito de aplicación, en el territorio de la Unión, se establecería para aquellos casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable (artículo 1.1).

En esa propuesta se distingue entre los sistemas de alto y bajo riesgo, estableciendo un régimen distinto de responsabilidad civil. A tal efecto, en el Anexo de la Resolución se incorporó una Lista de sectores de alto riesgo y de usos o fines de alto riesgo, facultando a la Comisión a modificar y ampliar dicha lista. Ese Anexo contiene una Lista exhaustiva y acumulativa, que enumera aquellos que conllevan un riesgo de violación de los derechos fundamentales y las normas de seguridad, por ejemplo, entre otros muchos, la conducción automatizada, o la gestión del tráfico.

Para los sistemas de IA de alto riesgo se establece una responsabilidad objetiva mediante la cual su operador será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA (artículo 4, que se remite al anexo de los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan). Al tratarse de un sistema objetivo, no se podrá eludir la responsabilidad alegando una actuación con la diligencia debida, o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA, sino únicamente en los supuestos de fuerza mayor (de conformidad con el artículo 4.3). Para evitar un conflicto en su aplicación, la propuesta de Reglamento europeo determina que este régimen de responsabilidad objetiva de los sistemas de IA prevalecerá sobre los regímenes nacionales de responsabilidad civil en el caso de que exista una calificación diferente. Acorde con el establecimiento de una responsabilidad sin culpa, se exige tanto al operador final de las operaciones como al operador

⁷⁷ Álvarez Olalla, P. (2021). Propuesta de reglamento en materia de responsabilidad civil por el uso de Inteligencia Artificial, del Parlamento Europeo, de 20 de octubre. *Revista Cesco*, N° 38, pp. 1-10. doi.org/10.18239/RCDC_2021.38.2742

inicial de los servicios de un sistema de IA de alto riesgo una garantía de cobertura mediante la suscripción de un seguro obligatorio de responsabilidad civil (artículo 4.5), en consonancia con los importes de las indemnizaciones contenidas en el Reglamento.

Paralelamente, junto a este régimen, para aquellos sistemas no considerados de alto riesgo se establece un sistema de responsabilidad subjetiva del operador por los daños o perjuicios causados por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA (artículo 8). En virtud de la misma, se exonera de responsabilidad al operador “si puede demostrar que no tuvo culpa en el daño o perjuicio causado, basándose en uno de los siguientes motivos: (a) el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador, o (b) se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles”. También impide que sea responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. Por lo tanto, en consonancia con este régimen, se establecen tres supuestos de exoneración de responsabilidad que corresponden a los presupuestos exigidos en un régimen de responsabilidad subjetiva: el caso fortuito, la actuación con la debida diligencia de un buen operador y la fuerza mayor. Con una excepción que contempla precisamente la autonomía controlada por el propio sistema, de manera que “el operador no podrá eludir su responsabilidad alegando que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA”.

Respecto a la intervención de un tercero en la causación del daño, mediante la interferencia en el sistema de IA por medio de una modificación de su funcionamiento o sus efectos, se establece la responsabilidad subsidiaria del operador, al recoger la propuesta normativa que será responsable del pago de una indemnización en el caso de que dicho tercero se encuentre ilocalizable o sea insolvente. Por último, en dicha propuesta de Reglamento se incorporan otros supuestos de imputación de la responsabilidad civil. En primer lugar, se regula el supuesto de concurrencia de culpas (a la que denomina negligencia concurrente), estableciéndose una reducción de la responsabilidad, de manera que “si el daño o perjuicio es causado por una actividad física o virtual, un dispositivo o un proceso gobernados por un sistema de IA o por la actuación de una persona afectada o de una persona de la que la persona afectada sea responsable, el alcance de la responsabilidad civil del operador con arreglo al presente Reglamento se reducirá en consecuencia” (artículo 10); así como

una exoneración de responsabilidad el caso de culpa exclusiva de la víctima o del perjudicados. Este precepto debe completarse con la regulación que establece sobre la “indemnización por la vía de regreso”, que posibilita la misma en proporción a su responsabilidad de otros operadores, la cual “se basarán en los respectivos niveles de control por parte de los operadores sobre el riesgo relacionado con la operación y el funcionamiento del sistema de IA”, debiéndose suplir la responsabilidad si no puede obtenerse de un operador responsable solidario la contribución que le sea atribuible.

La Resolución del Parlamento Europeo sobre la inteligencia artificial en la era digital (2022) también planteaba como necesaria una revisión de determinadas partes de las normas de responsabilidad existentes (esperando con interés, en este sentido, la presentación de una propuesta legislativa de la Comisión sobre la responsabilidad en materia de IA), y destacaba que la Directiva sobre responsabilidad por los daños causados por productos defectuosos y los sistemas nacionales de responsabilidad basados en la culpa pueden seguir siendo, en principio, la legislación central para contrarrestar la mayor parte de los daños causados por la IA⁷⁸.

En consonancia a esas necesidades y propuestas, la Comisión finalmente ha decidido elaborar una Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial (Directiva sobre responsabilidad en materia de IA), de 28 de septiembre de 2022⁷⁹, con el objeto de armonizar y actualizar las regulaciones nacionales sobre responsabilidad civil de los Estados en materia de IA, estableciendo unas normas específicas para los daños causados por los sistemas de IA para facilitar que las víctimas se vean resarcidas con una indemnización⁸⁰.

⁷⁸ Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_ES.html

⁷⁹ Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva de responsabilidad de IA) (COM(2022) 496 final. Disponible en : <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496>

⁸⁰ Entre los análisis de la propuesta de Directiva, se pueden destacar, entre otros: Fernández Hernández, C. (2022). La Comisión presenta una propuesta de Directiva sobre responsabilidad civil extracontractual en materia de IA, *Diario La Ley*, N° 65, 29 de septiembre de 2022; Muñoz Vela, J. M. (2023). IA y responsabilidad civil. Comentarios a las propuestas europeas en materia de derechos de daños por productos defectuosos y adaptación de las normas de responsabilidad civil extracontractual. *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 61; pp. 1-12.; Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret: Revista para el Análisis del Derecho*, n.º 3, pp. 55-100; Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi*

La propuesta ha puesto de relieve, tal y como ya indicaba el Libro Blanco sobre la IA, que las normas nacionales en vigor en materia de responsabilidad civil, particularmente las que se basan en la culpa, no son adecuadas para tramitar las reclamaciones de responsabilidad civil por daños causados por productos y servicios en los que se recurre a la IA. En este sentido, con arreglo a dichas normas, en nuestro caso conforme a la responsabilidad por culpa derivada del artículo 1902 del Código Civil, las víctimas deberían demostrar, a falta de normativa específica, la existencia de una acción u omisión negligente por parte de una persona que ha causado el daño. Las características específicas de la IA, incluidas su complejidad, su autonomía y su opacidad (el denominado *black box effect* o efecto de caja negra) dificultarían, entonces, determinar no solo el sujeto responsable, sino la prueba de que se cumplen los elementos precisos de la responsabilidad civil, fundamentalmente de la culpa y de la causalidad. Por ello, buscando la seguridad jurídica entre los Estados, antes de que estos adopten su normativa a los retos que plantea la IA en el régimen de la responsabilidad civil se ha aprobado esta propuesta de Directiva. Se trata de la primera propuesta de armonización específica de la normativa nacional sobre responsabilidad civil de la UE en el ámbito de la IA, para complementarla y modernizarla, introduciendo normas específicas para los daños causados por los sistemas de IA y para facilitar que las víctimas de daños relacionados con la IA puedan obtener una indemnización. De este modo, se aplicarían las normas nacionales, pero se deberán tener en cuenta en todos los Estados miembros, como mínimo, los mecanismos establecidos por la Directiva⁸¹.

Se introducen dos mecanismos fundamentales: primero, la “presunción de causalidad refutable” cuando parece razonablemente probable que exista un nexo de causalidad; por lo tanto, los tribunales estarían obligados a presumir que el resultado producido por el sistema de IA fue causado por culpa del proveedor de IA. No es que se requiera menos prueba, sino que es cuestión de nexo causal probabilístico; de este modo, se faculta al juez para que pueda, atendiendo a las circunstancias, presumir el nexo causal entre la acción culposa y la información o falta de información del sistema⁸². Por otro lado,

Doctrinal, n.º 4, pp. 1-9; y Ortiz Fernández, M. (2024). La «adaptación» del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad, *IDP*, n.º 40, pp. 1-12, <https://raco.cat/index.php/IDP/article/view/n40-ortiz>.

⁸¹ “Así pues, los tribunales de los estados, al resolver los pleitos sobre responsabilidad, aplicarán las respectivas disposiciones nacionales, pero teniendo en cuenta las reglas y presunciones de la mencionada propuesta de Directiva”. Ortiz Fernández, M. (2024). La «adaptación» del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad civil, op. cit., p. 5.

⁸² Martín Casals, M. (2023), Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, n.º 3, p. 73 . <https://doi.org/10.31009/InDret.2023.i3.02>.

se incorpora un derecho de acceso a las pruebas de empresas o proveedores, cuando se trata de IA de alto riesgo. Por lo tanto, un tribunal puede ordenar a un proveedor de un sistema de inteligencia artificial de alto riesgo que revele las pruebas relevantes y necesarias sobre su producto. Asimismo, estas solicitudes también se pueden realizar a terceros en casos específicos. De este modo, la propuesta contribuye al cumplimiento de los requisitos para sistemas de IA de alto riesgo impuestos por la Ley de IA.

Además, la propuesta incorpora adaptaciones de la responsabilidad del productor, en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos para los supuestos de reclamaciones que se generan en ese contexto. De ese modo, se trata de cubrir ambos ámbitos, el de la responsabilidad por los daños causados por productos defectuosos, que cubre la responsabilidad objetiva del productor, y el de las demandas de responsabilidad fundamentadas principalmente en la culpa.

Entiendo que, al ser una normativa exigible de mínimos, ello no impide una regulación nacional más exigente en función del sector de actividad, como sucede en los supuestos de vehículos autónomos, donde la aplicación de la LRCSCVM, en la que se imputa la responsabilidad al conductor, y en su defecto al propietario, en función del riesgo, opera otorgando una mayor protección a la víctima, como ya hemos visto, con unos resultados más favorables que las meras presunciones en la carga probatorias que ofrece la propuesta de Directiva en favor de dichas personas. Únicamente, respecto a los daños materiales el régimen ofrecido pudiera resultar beneficioso, debido a que el régimen de responsabilidad es distinto al de los daños personales; al igual que sucede cuando el accidente fuera debido a un producto defectuoso, donde el criterio de imputación de la responsabilidad derivada del TRLGDCU o de la Directiva establece una mayor protección a víctimas y perjudicados.

6. HACIA UN NUEVO CRITERIO DE RESARCIMIENTO DE DAÑOS DERIVADO DE LA AUSENCIA DEL CONDUCTOR DEL VEHÍCULO

No cabe duda de que los sistemas de IA, mediante diferentes tecnologías de sistemas avanzados de asistencia al conductor (ADAS), ofrecen muchas ventajas, entre otras, posibilita la reducción del número de siniestros. Ahora bien, aunque se espera que las prestaciones de estos vehículos inteligentes autónomos se realicen conforme a las especificaciones de su diseño, también lo es que se produzcan errores y fallos mecanismos imprevistos en su uso, en ocasiones, incluso, la propia opacidad de los algoritmos pueden dificultar conocer el modo en que han actuado. Nos encontramos con una problemática que

abarca un amplio elenco de elementos, que afectan desde el nexo causal, la culpabilidad o la imputación de la responsabilidad hasta los mecanismos aseguradores. De este modo, un mal funcionamiento, una falta de actualización o, incluso, un ataque a la transmisión de la información de estos vehículos puede provocar daños de diversa índole. Estos daños, sean materiales o personales, pueden estar vinculados, por lo tanto, a una gran variedad de riesgos.

Hemos llegado a un punto de inflexión en el que debemos plantearnos si buscar un nuevo marco normativo para dar respuesta a los vehículos autónomos dotados de IA, que se encuentran en pleno desarrollo, o plantearnos si es suficiente con adaptar los recursos legales existentes. La nueva casuística, que emerge especialmente con la autonomía creciente de los robots, abre un nuevo espacio teórico y práctico sobre la responsabilidad derivada de los que se sirven de los sistemas de IA, máxime al existir diferentes criterios de imputación de la responsabilidad⁸³.

Un elemento necesario para que surja la responsabilidad civil es la existencia de una relación causa-efecto entre el daño y el hecho que lo produjo. En efecto, debe existir un nexo causal entre la acción u omisión (primer presupuesto) y el daño producido (segundo presupuesto), aunque en ocasiones los tribunales lo resuelven como un problema de causalidad aunque realmente sea de negligencia, y viceversa. La exigencia de dicho requisito no puede resultar alterada por la aplicación de la teoría del riesgo o la existencia de una responsabilidad objetiva, es decir, para que se impute la responsabilidad, cualquiera que sea el criterio que se utilice (con base en la culpa o el riesgo), es requisito indispensable la determinación del nexo causal entre la conducta del agente y la producción del daño. En relación a dicha causalidad, es necesario determinar qué causa es relevante para poder establecer la imputación del daño a un determinado sujeto. Es la teoría jurídica de la causalidad adecuada la que tradicionalmente se ha tomado como válida para imputar la responsabilidad, que apunta a que no todos los hechos concurrentes al daño son causa suficiente sino que únicamente pueden ser considerados como causas de un perjuicio los acontecimientos apropiados para producir el concreto resultado dañoso⁸⁴; sin embargo, desde otras perspectivas se entiende que lo relevante no es solo

⁸³ Monterroso Casado, E. (2022). Análisis de la imputación de la responsabilidad profesional en el nuevo escenario de la inteligencia artificial. En A. Muñoz Villareal (dir.), *Derecho de los Riesgos Tecnológicos*, EOLAS, Madrid, pp. 201-234.

⁸⁴ Sobre la causalidad jurídica, véase Díez-Picazo, L. (1999). *Derecho de Daños*, Civitas, Madrid, pp. 341-345; y Reglero, F. (2004). *Tratado de Responsabilidad Civil*, Aranzadi, Pamplona, p. 390. Para un análisis más exhaustivo, Arcos Vieira, M. L. (2005). *Responsabilidad civil: nexo causal e imputación objetiva en la jurisprudencia*, Aranzadi, Pamplona.

la causación un daño, sino el haber originado cierto riesgo para que este se produzca⁸⁵.

En este escenario, nos encontramos con la dificultad de delimitar la causa del daño, por un lado, y el criterio de imputación de la responsabilidad por otro, ya que no es equiparable un daño como consecuencia de un error en el sistema, de la incorrecta utilización por un sujeto, por la ausencia de una actualización, por una falta de mantenimiento del propietario (sea empresa o persona física), un acontecimiento externo (como un ataque informático o una avería en el suministro de energía) o una causa desconocida. Además, a medida que incrementa la autonomía, las causas pueden derivar de una interacción de agentes (ingeniería mecánica, electrónica, tecnología de la información y software incorporado), lo que dificulta la delimitación del sujeto que debe soportar el daño. Por otro lado, se presenta el problema de la prueba de la causa que originó el daño, y si esta fue debida a la actuación negligente de uno o varios de los sujetos intervinientes, a un caso fortuito o a una fuerza mayor, o a una concurrencia de acontecimientos. Si a todo ello añadimos que, en ocasiones, su operatividad exige la presencia de redes artificiales neuronales, la dificultad de localizar al responsable puede resultar compleja⁸⁶.

Ante las dificultades de detectar la causa del accidente en un marco ya de por sí complejo, donde coexisten los vehículos autónomos y donde el error humano también puede intervenir⁸⁷, y por lo tanto de identificar al sujeto responsable, debemos analizar si la responsabilidad debería recaer en el dueño del vehículo, en el operador, en el productor o en el diseñador del sistema de IA, teniendo en cuenta, con ello, que su regulación debe aparejar una solución a la reparación de los daños que se puedan causar por los vehículos

⁸⁵ Según el AED, “el criterio fundamental para imputar un daño a una conducta es el del incremento del riesgo, el de si esa conducta, en el momento de realizarse (ex ante), elevaba el riesgo del resultado dañoso que finalmente se materializó. Imaginemos una conducta negligente que ex ante aumenta el riesgo de que se produzca el accidente luego considerado por el juez. Pongamos, por ejemplo, que el conductor de un autobús circula con él a una velocidad excesiva, lo que eleva la probabilidad de chocar frontalmente con un árbol caído en la vía pública, evento que finalmente ocurre. Si las personas que se encuentran en una situación como ésta no respondieran de los daños derivados de semejantes accidentes, sus incentivos para respetar los límites de velocidad serían seguramente insuficientes, lo que daría lugar a que el número de aquellos choques fuera demasiado elevado. Es por ello que conviene que se les imputen tales daños”. Y a estos efectos, una solución contraria distorsionaría en mayor grado los incentivos de los potenciales responsables para actuar con cuidado, Doménech Pascual, G. (2019). Sobre el poder explicativo del análisis económico del Derecho. En especial, del Derecho de daños. *InDret*, n.º 2, p. 21. <https://indret.com/wp-content/uploads/2019/07/1465-pdf>

⁸⁶ Monterroso Casado, E. (2019). Repercusiones de la inteligencia artificial en el ámbito de la responsabilidad civil. *Revista de responsabilidad civil, circulación y seguro*, n.º 11, p. 12.

⁸⁷ Steege, H. et al. (2024). Autonomous Vehicles and Civil Liability in a Global Perspective., Springer, p. 5.

autónomos, con una visión práctica que ofrezca soluciones eficaces a víctimas y perjudicados.

Si el operador puede asumir las funciones de controlar el vehículo, considero que debe equipararse su figura a la del conductor tradicional, respondiendo en caso de que se ocasionen daños⁸⁸. El problema entiendo que se produce cuando se carece de dicho control y donde es preciso que la doctrina proporcione argumentos y soluciones para ser valoradas a la hora de imputar la responsabilidad o quién debe afrontar los daños causados por los vehículos autónomos, sin perjuicio de la suscripción de un seguro para tales casos.

La cuestión es encontrar quién se hará cargo del resarcimiento del daño. Existen distintas propuestas o posibilidades, que pasan por el propietario del vehículo autónomo, el conductor u ocupante del mismo, la empresa fabricante de automóviles, el proveedor o el operador del software, el propio vehículo autónomo si tuviera personalidad jurídica propia, o la compañía de seguros. Y tampoco faltan opiniones que consideran que la regulación de los vehículos autónomos debe realizarse instaurando un régimen completamente nuevo o bien efectuando una relevante revisión de la LRCSCVM.

A continuación, vamos analizar las posturas principales de quién se considera que debe cubrir el coste de los accidentes, y que se apoyan con argumentos de distinta índole: la responsabilidad del fabricante; la responsabilidad del propietario; la responsabilidad del operador del vehículo; y la reparación por parte de la aseguradora del vehículo, tomando como referencia la LRCSCVM o sin imputación de la responsabilidad.

6.1. RESPONSABILIDAD DEL FABRICANTE DEL VEHÍCULO

Bajo esta postura, el fabricante debería ser enteramente responsable si se considera al vehículo autónomo un producto defectuoso. Ahora bien, si se pretende esa imputación de los daños causados al fabricante, entendiendo que el daño ha sido causado por un producto defectuoso debería modificarse la ley para incorporar esa producción del daño del vehículo autónomo. Así lo señala Núñez Zorrilla, “si estamos hablando de una responsabilidad que no nace de la negligencia del fabricante, sino de una actuación incorrecta producto de una decisión autónoma de la máquina, entonces las nociones de

⁸⁸ En este sentido, el hecho de que un robot (como entendemos que pudiera ser, entonces, un vehículo autónomo), permanezca vinculado a la acción humana resulta relevante para la imputación de la responsabilidad al mismo. Véase Ebers, M. (2016). La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil?, op. cit., p. 8.

defecto y de producto defectuoso deberían modificarse para adaptarse a esta nueva forma de producción del daño⁸⁹.

Fuera de nuestras fronteras es donde más vamos a encontrar esa postura que aboga por la responsabilidad del fabricante en lugar de la responsabilidad del propietario del vehículo, argumentando que el fabricante tiene control operativo sobre el vehículo autónomo, mientras que el propietario es solo el ocupante. Además, se sostiene que el fabricante se encuentra en la mejor posición para decidir qué invertir en el sistema operativo para evitar accidentes; y también se considera que con esta medida se incentiva al fabricante a investigar formas de mejorar el sistema, sin olvidar que puede internalizar el coste del accidente en el precio del vehículo⁹⁰.

Otros autores, sin embargo, prefieren apoyarse en el sistema de responsabilidad por productos defectuosos y trasladar la responsabilidad a los fabricantes, debiéndose incrementar su nivel de diligencia y cuidado, considerándolos como un transportista de pasajeros, entendiendo que serían responsables, incluso de la más mínima negligencia⁹¹; o abogando por un régimen de responsabilidad totalmente objetiva del fabricante sobre la base de que la nueva tecnología les convierte en evitadores de los accidente que resultan del uso de estos productos, y acelerará el progreso técnico y la seguridad⁹². Cabe preguntarse si, entonces, ello no reduciría el deber de diligencia del operador, en especial cuando tiene la posibilidad de retomar el control del vehículo. Por otro lado, no debemos olvidar que la responsabilidad del fabricante solo podría entenderse, conforme a la normativa actual, si el daño ha sido causado por un producto defectuoso, donde, tras las modificaciones de la directiva europea, se incluirían los sistemas de IA. Y que, además, obligaría a los fabricantes a la

⁸⁹ Núñez Zorrilla, M.^a C. (2021). Los nuevos avances en la regulación europea de la responsabilidad civil por los daños ocasionados en el ámbito del transporte con inteligencia artificial. *Revista Europea de Derecho Europeo*, núm. 78-79, p. 214. https://doi.org/10.37417/REDE/num78-79_2021_636.

⁹⁰ Abraham, K. and Robert L. Rabin, R. (2019). Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era". *Virginia Law Review*, vol. 105, pp. 127-171. https://www.virginialawreview.org/wp-content/uploads/2020/12/A&R_Book.pdf. De hecho, estos autores sostienen que hasta que los niveles de autonomía SAE 4 o 5 alcanzan el 25% de los vehículos en circulación se debería implantar la responsabilidad empresarial del fabricante por productos defectuosos en los accidentes en los que se vieran implicados estos vehículos, que no fueran daños materiales, y que cuando se superara ese umbral abogan por aplicar ya el sistema de responsabilidad sin culpa, solo que existiera una clara negligencia del propietario del vehículo (p. 132). Postura que no es compartida por la mayoría de la doctrina.

⁹¹ LeValley, D.. (2013). Autonomous Vehicle Liability-Application of Common Carrier Liability. *Seattle University Law Review*, Vol. 36, pp. 5-26. <https://core.ac.uk/download/pdf/235988125.pdf>

⁹² Rapaczynski, A., (2016). Driverless Cars and the Much Delayed Tort Law Revolution. *Columbia Law and Economics Working Paper* No. 540, 2016, pp. 1-36. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764686.

suscripción de un seguro obligatorio de daños de los vehículos autónomos que se pusieran en circulación, lo que traslada el ámbito de aseguramiento del vehículo al fabricante, aumentando la complejidad de las reclamaciones cuando ya existe en nuestro ordenamiento una extensa regulación y entramado eficiente respecto a la reparación de los daños causados por los vehículos a motor. Por todo ello, no nos mostramos partidarios de un régimen general, a priori, de responsabilidad del fabricante, sin perjuicio de la posibilidad de repetición por las asegurados de los vehículos cuando exista, o se presuma, conforme a los nuevos mecanismos probatorios de la próxima normativa europea, la existencia de un defecto. Además, aunque la normativa europea cree presunciones para facilitar la prueba del defecto, no deja este de constituir un elemento necesario para la imputación de la responsabilidad; y, en el caso de vehículos autónomos, ello implica unos conocimientos precisos y específicos sobre esta avanzada tecnología, que requeriría informes de expertos⁹³.

En nuestra opinión, es el seguro obligatorio del vehículo, y no el del fabricante, el que debe indemnizar a la víctima, sin que esta tenga la carga de probar el fallo del vehículo. Y ello incluso aunque pudiera probar la relación de causalidad entre el defecto del vehículo autónomo y el daño⁹⁴. Dicha facultad estará en mano de la aseguradora para repetir si se apreciara la misma contra el fabricante tanto si se tratan de defectos de fabricación, de diseño o de información. De este modo, el fabricante sería responsable por accidentes causados por un mal funcionamiento del hardware, por una equivocación en el diseño del software, o un fallo del sistema operativo debido a un error de programación. En el caso de los defectos de información, sería preciso diferenciar entre que dicho defecto fuera debido a que los sensores no transmiten correctamente la información, por ejemplo, por un fallo del LIDAR, del dispositivo de detección láser, de los dispositivos de señalización de tráfico; que exista un fallo en el entorno operativo de la señal de tráfico, de los operadores de telecomunicaciones, o de los gestores de infraestructuras de transporte inteligentes. Incluso la propia administración pública puede ser la responsable

⁹³ En esta línea, véase Van Uytsel, S. (2021). Different Liability Regimes for Autonomous Vehicles: One Preferable Above the Other? En S. Van Uytsel, y D. Vasconcellos Vargas (Eds.) *Autonomous Vehicles*, Springer, 2021, pp. 71 y 72. La complejidad de fabricación de los vehículos autónomos y la complejidad del proceso de reclamación también es puesto de relieve por González Alonso, A. (2021). Responsabilidad civil y vehículos de conducción autónoma. ¿o no? En E. Llamas Pombo, J. Arrubla Paucar y C.I. Jaramillo (Dirs). *Derecho de daños y protección de la persona*, Tirant lo Blanch, Valencia, pp. 215-220.

⁹⁴ Sostiene Castells i Marqués que la dificultad la víctima de probar la relación de causalidad entre el defecto y el daño sufrido (artículo 139 LGDCU) “resultará minorada, gracias a las cámaras instaladas en el vehículo y a los archivos de datos electrónicos (como equivalentes a las cajas negras d los aviones), los cuales proporcionarán información relevante del accidente”. Castells i Marqués (2017). Vehículos autónomos y semiautónomos. En S. Navas Navarro (coord.). *Inteligencia artificial, Tecnología, Derecho*, Tirant lo Blanch, p. 115.

de la infraestructura de la vía o de las señales que puedan estar deterioradas, siendo, en esos casos, el responsable contra el que podría repetir la aseguradora, y no ya el fabricante. De este modo, hay que descartar la idea que que los fabricantes respondan a priori por el funcionamiento de los vehículos autónomos ya que ello supondría un obstáculo a la implantación en nuestra carreteras de estos vehículos⁹⁵.

6.2. RESPONSABILIDAD DEL OPERADOR O DEL PROPIETARIO DEL VEHÍCULO

El Anexo I de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial define como conductor a la persona que “maneja el mecanismo de dirección o va al mando de un vehículo”, señalando el artículo 13, relativo a las normas generales de conducción, que “el conductor debe estar en todo momento en condiciones de controlar su vehículo”⁹⁶. Aunque en nuestra legislación aún no se permita la conducción autónoma, existe un proyecto legislativo en materia de conducción automatizada con modificaciones al Reglamento General de Vehículos en el que, como hemos visto, se incluyen los conceptos de operador a bordo y operador remoto. Una propuesta podría ser la ampliación del concepto de conductor, que se podría transformar en operador del vehículo autónomo⁹⁷. Es cierto que la LRCSCVM también permite la imputación al propietario, cuya fórmula entiendo que debe seguir manteniéndose, para posibilitar la reclamación de los daños. En este sentido, el artículo 1.3 de la LRCSCVM establece un supuesto de responsabilidad por hecho ajeno, la del propietario del vehículo por la actuación del conductor. Este precepto remite a la norma general del artículo 1903 del CC, que establece una responsabilidad directa por las actuaciones de los dependientes que son causa del daño. Se trata de una responsabilidad civil directa, que cesará cuando el mencionado propie-

⁹⁵ Indica a este respecto Elizalde que “pretender que los fabricantes respondan por todos los daños causados por el funcionamiento del vehículo, independientemente de su causa, plantea algunas limitaciones para la innovación y el desarrollo de estos vehículos. Podría provocar que los fabricantes no quisieran comercializar sus vehículos hasta que considerasen que son los suficientemente seguros para no tener ningún accidente (cuando la probabilidad de tener un accidente sea aproximadamente cero). Consecuentemente, la comercialización de este tipo de vehículos se prolongaría, perdiendo la sociedad los beneficios netos de tener estos vehículos antes en las carreteras”. Elizalde Salazar, I. (2022), *Vehículos autónomos. Responsabilidad civil y seguro*, op. cit., p. 135.

⁹⁶ En el mismo sentido, señala la DGT que todos los vehículos que circulan por la vía pública necesitan un conductor, siendo el conductor “la persona que maneja el mecanismo de dirección o va a los mandos DGT (2014). Definición de conductor. En *Los conductores principios fundamentales del tráfico*, p. 7. https://www.dgt.es/export/sites/web-DGT/.galleries/downloads/conoce_la_dgt/qu-hacemos/educacion-vial/adultos/no-formal/conductores.pdf

⁹⁷ Castells i Marquès, M. (2017). Vehículos autónomos y semautónomos, op. cit., p. 112.

tario pruebe que empleó toda la diligencia de un buen padre de familia para prevenir el daño. No obstante, esta facultad de exoneración es interpretada en todos los supuestos del artículo 1903 CC de manera muy estricta por la jurisprudencia. Y, por otro lado, la responsabilidad será subsidiaria en los supuestos de responsabilidad derivada del artículo 120.5 del Código Penal. Por eso, otra propuesta para el caso de los vehículos autónomos es que no se exija la existencia de esa relación de dependencia entre conductor y propietario para dar cabida a muchos de los supuestos que se darán con el avance e implantación de los vehículos de conducción autónoma (en servicio de *car sharing* o robotaxis).

Ahora bien, la postura que hemos encontrado que cuenta con mayores adeptos es la que defiende la responsabilidad del propietario del vehículo autónomo, aunque los argumentos empleados y el modo de llevar a cabo la misma difiere. Arévalo y Murga señalan que la responsabilidad, en ausencia de conductor, en virtud del principio *pro damanato*, vigente en el derecho español, debe recaer en el propietario del vehículo, y su responsabilidad debe interpretarse como responsabilidad objetiva, y en la compañía aseguradora o, en su caso, en el Consorcio de Compensación; y si el siniestro se debiera al defecto del vehículo, en cualquiera de sus facetas, el propietario podría reclamar contra el fabricante⁹⁸. Torroba, por su parte, indica que debe regularse “la responsabilidad civil del propietario o la persona, física o jurídica, que se sirva del vehículo, en función del beneficio que el mismo reporta, a falta de un conductor al que imputar la culpa”⁹⁹. Bajo esta premisa, se quiere dejar al margen al conductor, ya que al contar los vehículos con capacidad para analizar las situaciones y definir las actuaciones, sin previo control ni dirección de una persona física, implicaría la exoneración de responsabilidad por dicha actuación, salvo que el pasajero al volante hubiera podido convertirse en conductor y evitar el daño tomando el control del vehículo. Esta facultad guarda consonancia con el Proyecto de reforma del Reglamento General de Circulación, que ya analizamos¹⁰⁰. Sin embargo, la solución puede ser incluso más compleja o dar lugar a otras respuestas en el caso de los vehículos de nivel 3, donde el conductor puede tomar el control, desactivando el sistema de IA. La imputación de

⁹⁸ Fernández Arévalo, A. y Murga Fernández, J.P. (2024). Civil Liability for Damage Caused by Autonomous Vehicles Under Spanish Law. En H. Steege et al., *Autonomous Vehicles and Civil Liability in a Global Perspective*, Springer, pp. 345-359.

⁹⁹ Torroba Díaz, J. (2019). Los vehículos autónomos y la responsabilidad del fabricante. *Revista de Responsabilidad Civil y seguro*, n.º 55, p. 25.

¹⁰⁰ El Proyecto de reforma del Reglamento General de Circulación, en el nuevo Anexo V, propone que los sistemas de conducción automatizada, una vez activados, deben ser capaces por sí mismos de: “g) Poder ser desactivado en cualquier momento por un operador autorizado. h) En caso de desactivación, el sistema deberá asegurar que el operador puede tomar el control de forma segura y efectiva. En su defecto, el sistema de conducción automatizada deberá llevar el vehículo de forma independiente al estado de riesgo mínimo. i) Indicar al operador remoto, si existiera conforme a sus condiciones de uso, la necesidad de activar una maniobra de conducción alternativa sobre el vehículo, la desactivación del sistema con suficiente tiempo de respuesta, o la activación de las señales necesarias”.

la responsabilidad podría, bajo ese punto de vista, verse comprometida. Dicho esto, no olvidemos que el actual régimen de responsabilidad por daños personales causados es objetivo, prescindiendo de cualquier negligencia, salvo la de la culpa exclusiva de la víctima e, incluso, se prescinde de cualquier tipo de reproche culpabilístico en función de si la víctima es capaz de culpa civil.

Tampoco faltan opiniones a favor de la apreciación de una concurrencia de responsabilidades¹⁰¹. Téngase en cuenta que los vehículos autónomos operan con sistemas en conexión, no solo con los propios dispositivos, sino que se ven inmersos en ese entramado las infraestructuras de carretera, el almacenamiento y procesamiento de datos y otros participantes que también actúan en el tráfico. Al congregarse productos, servicios y comportamientos de diferente índole, podría confluír la combinación de diferentes regímenes de responsabilidad, lo que dificultará el resarcimiento de la víctima. Por ello, “una ventanilla única” puede facilitar la obtención de una compensación¹⁰². La indemnización sin culpa es la propuesta que realizamos ya que lo contrario no reportaría un beneficio ni eficiencia en el sistema de reparación del daño en aras a la protección a la víctima.

En la doctrina internacional, encontramos también distintos argumentos para que los propietarios de vehículos autónomos sean los responsables. Una de ellas es estableciendo una analogía de la propiedad de este tipo de vehículo autónomo con las consecuencias de tener un animal peligroso como mascota, que piensa y actúa independientemente de sus dueños humanos, y que causa unos daños o lesiones; también se ha sostenido que se impute la responsabilidad por los daños si el vehículo se encuentra bajo la custodia del propietario; y algún académico aboga por la protección de los fabricantes, aplicando la teoría de la asunción del riesgo¹⁰³. También se ha apuntado, creemos que aquí ya con más acierto, la imputación al propio conductor/pasajero, por su naturaleza y su capacidad para

¹⁰¹ “Esta responsabilidad del operador, sin embargo, no será absoluta, sino que se verá modulada o disipada, e incluso compartida con otros sujetos (piénsese en el fabricante del sistema de IA, en el del vehículo o incluso en las aseguradoras de la responsabilidad civil), en atención a las circunstancias en las que se haya producido el siniestro”. López Mas, P. J. (2024). La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento, op. cit., p. 85.

¹⁰² Van Uytsel, S. (2021). Different Liability Regimes for Autonomous Vehicles: One Preferable Above the Other? En *Perspectives in Law, Business and Innovation*, Springer. pp. 67-92.

¹⁰³ Véase la recopilación de estas distintas posturas y argumentos de la doctrina que recogen Rosemadi, J. F., Khong, D. W. K., & Radhakrishna, G. (2022). Civil Liability of Autonomous Vehicles: A Review of Literature. *IJUM Law Journal*, núm. 30 (2), pp. 155-179. <https://doi.org/10.31436/ijumlj.v30i2.740>; y Kubica, M. L. (2022). Autonomous Vehicles and Liability Law. *The American Journal of Comparative Law*, Vol. 70, pp. 139-169. <https://doi.org/10.1093/ajcl/avac015>

prevenir el accidente, incluso, con argumentos de analogía con los supuestos de accidentes aéreos cuando el avión opera con el piloto automático activado¹⁰⁴.

6.3. RESARCIMIENTO DEL DAÑO POR LA ASEGURADORA DEL VEHÍCULO, TOMANDO COMO REFERENCIA LA LRCSCVM

No faltan opiniones como la nuestra a favor de la aplicación de la LRCSCVM¹⁰⁵. Este sistema, como hemos visto, facilita la reparación del daño personal aunque se produzca un defecto del vehículo, al establecer el artículo 1.1, en su segundo párrafo de la Ley que “no se considerarán casos de fuerza mayor los defectos del vehículo ni la rotura o fallo de alguna de sus piezas o mecanismos”. Además, el hecho de que estos vehículos sean más seguros no puede implicar alejarnos del criterio de imputación en virtud del riesgo¹⁰⁶. Y ello, sin perjuicio de que, como hemos apuntado, por diversos motivos, sea preciso extender este régimen también a los daños materiales¹⁰⁷.

Sin perjuicio de que los supuestos de daños causados por productos que integren sistemas de IA como los vehículos autónomos puedan encuadrarse en la normativa de las propuestas de directivas por productos defectuosos o en la relativa a la responsabilidad en materia de IA, entiendo que el marco correcto de referencia debería seguir siendo la LRCSCVM, en cuanto se trata de una amplia regulación sectorial de los supuestos de daños causados en

¹⁰⁴ Pearl se pregunta que si analógicamente no sería el “conductor” de un vehículo autónomo como el maquinista de un tren o el piloto de un avión en “piloto automático”, o si es simplemente un pasajero, con poco o ningún control sobre el comportamiento del vehículo. *Pearl, T. (2019). Alternative Victim Compensation Schemes. William & Mary Law Review*, Vol. 60, n° 5, 2019, p. 1855. <https://wmlawreview.org/sites/default/files/Pearl.pdf>

¹⁰⁵ Seijo Bar, A. (2020). El coche autónomo: una aproximación a la responsabilidad civil en la era digital. En E. Ortega Burgos (dir.), *Nuevas tecnologías*, Tirant lo Blanch, Valencia, p. 373; Álvarez Olalla (2019). Responsabilidad civil en la circulación de vehículos autónomos”. En E. Monterroso Casado (dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Valencia, Tirant lo Blanch, p. 164; Navarro-Michel (2020) La aplicación de la normativa sobre accidentes de tráfico a los causados por vehículos automatizados y autónomos. *Cuadernos de Derecho Transnacional*, Vol. 12, N° 1, p. 942; o López Mas. P.J. (2024). La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento. *RCDI*, n.º 801, p. 85.

¹⁰⁶ En este sentido señala Navarro-Michel (2020) que “la responsabilidad objetiva debe continuar acompañando a los vehículos, sean convencionales o automatizados, en aras a la protección de la víctima”. Vehículos automatizados y responsabilidad por producto. *Revista de Derecho Civil*, vol. VII, n° 5, .p. 210.

¹⁰⁷ Esta posición ya he apuntado que ya la he defendido en otras ocasiones, con independencia del vehículo, y con mayor justificación aún en el caso de vehículo autónomos. A favor de esa extensión del régimen de responsabilidad objetiva los daños materiales causados por vehículos autónomos, véanse también Navarro-Michel, M. (2020). Vehículos automatizados y responsabilidad por producto. *Revista de Derecho Civil*, vol. VII, n° 5, .p. 211; y Álvarez Olalla, P. (2017). Desafíos legales ante la circulación de los coches autónomos: implicaciones éticas, responsabilidad por accidente y ciberseguridad. *Revista Doctrinal Aranzadi Civil-Mercantil*, n° 2, pp. 129-138.

accidentes de circulación y de su aseguramiento. Y ello dejando a salvo que deberían introducirse reformas precisas en dicha legislación que vayan adaptándola a la normativa europea tanto sobre la IA como a la relativa a productos defectuosos¹⁰⁸. Igual que está sucediendo con la reglamentación de otros ámbitos específicos, resulta conveniente una regulación específica en este ámbito, con unas premisas comunes, que entiendo que debería contenerse en la LRCSCVM, modificando la misma para adaptarla a este tipo de conducción, siendo necesaria una legislación específica a nivel de la UE en el sector los vehículos sin conductor -como ya ocurre con los drones (vehículos autónomos aéreos), que no contaban con una detallada y específica regulación -, para evitar que los Estados miembros regulen estos aspectos de forma independiente y produzcan criterios jurídicos fragmentados¹⁰⁹.

Igual que cuando acontece un accidente causado por un vehículo convencional acudimos al criterio de imputación de la responsabilidad previsto en la LRCSCVM, que hace recaer al conductor la responsabilidad por los daños causados, y por lo tanto a la aseguradora que cubre el riesgo, sin importarnos si la causa del daño se debió a que el vehículo que se conducía tuviera algún defecto (un fallo en los frenos o en la suspensión, o un bloqueo de la dirección) o anomalía (resultante del propio estado del vehículo, sin que sea imputable al fabricante, sino a la falta de mantenimiento), como sucede en un porcentaje de los casos¹¹⁰, y sin perjuicio de que la compañía del seguro del vehículo pueda entablar una acción de responsabilidad contra el fabricante del vehículo, en virtud del artículo 10 de la LRCSCVM¹¹¹. Así ocurriría también en

¹⁰⁸ “Si bien es preferible una reglamentación sectorial específica para la amplia gama de posibles aplicaciones, era necesario contar con un marco jurídico horizontal basado en principios comunes, con el fin de establecer una igualdad de normas en toda la Unión y proteger eficazmente nuestros valores europeos. Es preferible que estas nuevas normas comunes para los sistemas de IA adopten la forma de reglamentos, que son las disposiciones normativas con más capacidad para adaptarse a la evolución del ámbito digital, que se caracteriza por una rápida dinámica transfronteriza”. Núñez Zorrilla, M.^a C (2021). Los nuevos avances en la regulación europea de la responsabilidad civil por los daños ocasionados en el ámbito del transporte con inteligencia artificial, op. cit., p. 250.

¹⁰⁹ Monterroso Casado, E. (2024). *Robots and Liability: New Criteria and Attribution Methods*. En Moura Vicente, D., Soares Pereira, R., Alves Leal, A. (eds) *Legal Aspects of Autonomous Systems*. Springer, pp. 133-134.

¹¹⁰ De hecho, según datos de la AECA-ITV (2022), en más de un cuarto de los accidentes de tráfico, al menos uno de los vehículos implicados en el siniestro presentaba algún tipo de anomalía o fallos mecánicos en su funcionamiento. https://www.aeca-itv.com/wp-content/uploads/2022/12/2022_12_21-NP-defectos-y-siniestros-viales-ok.pdf (fecha de consulta 20/09/2024). Ahora bien, es preciso que apuntemos que ello no quiere decir que estos fallos sean imputables al fabricante, sino que muchos son ocasionados por la propia antigüedad del vehículo y su estado de conservación.

¹¹¹ Señala el artículo 10 la facultad de repetición del asegurador, una vez efectuado el pago de la indemnización, contra: (a) El conductor, el propietario del vehículo causante y el asegurado, si el daño causado fuera debido a la conducta dolosa de cualquiera de ellos o a la conducción bajo

el supuesto de que el accidente sea debido a la conducta negligente de otro usuario de la vía. Álvarez Olalla considera que en los accidentes imputables a terceros, el seguro cubriría el daño, pero posteriormente podría repetir, al igual que si un hacker interfiere en el sistema de IA del vehículo¹¹². Del mismo modo, si la causa del accidente se debe a un defecto del software que ocasiona que el vehículo tome una decisión equivocada, con independencia del nivel de autonomía del vehículo y la posible contribución al accidente por falta de supervisión del conductor, la aseguradora que hará frente a la indemnización podrá repetir contra el fabricante.

Otros autores han apuntado que esto dará lugar a una segunda reclamación, la de la aseguradora contra un tercero (entendemos que el fabricante) para el reintegro de la indemnización, con un incremento de los litigios¹¹³. Ahora bien, esta facultad de repetición no siempre será tan sencilla, al menos si se utiliza el argumento del producto defectuoso, en la medida que estos vehículos puedan estar dotados de redes neuronales artificiales para aprender de datos mediante el *deep learning* (que analiza inmensas cantidades de datos para detectar patrones y anomalías en el rendimiento del vehículo) y el *machine learning* (o aprendizaje automático, que permite a las máquinas, en este caso a los vehículos, aprender de forma autónoma mediante el análisis de datos y la identificación de patrones). Es por ello que entiendo que es preciso una regulación específica de esa posibilidad de repetición. Esperemos que el menor número de accidentes causados por estos sistemas inteligentes unido a un criterio regulatorio claro de reparación del daño conlleve un descenso de los litigios y un incremento de la seguridad jurídica.

6.4. RESARCIMIENTO DEL DAÑO POR LA ASEGURADORA DEL VEHÍCULO, SIN IMPUTACIÓN DE LA RESPONSABILIDAD

Bajo esta postura, sería la aseguradora del vehículo la que debe resarcir el daño para lo que se precisa de un cálculo de las primas de seguro para hacer frente a tales riesgos. Para Geistfeld, con el despliegue masivo de los vehículos autónomos, cambiará todo el sistema de conducción, que pasará de un com-

la influencia de bebidas alcohólicas o de drogas tóxicas, estupefacientes o sustancias psicotrópicas; (b) el tercero responsable de los daños. c) Contra el tomador del seguro o asegurado, por las causas previstas en la LCS, y, conforme a lo previsto en el contrato, en el caso de conducción del vehículo por quien carezca del permiso de conducir; y (d) en cualquier otro supuesto en que también pudiera proceder tal repetición con arreglo a las leyes.

¹¹² Álvarez Olalla, P. (2019). Responsabilidad civil en la circulación de vehículos autónomos, op. cit., p. 167.

¹¹³ Torroba Díaz, J. (2019). Los vehículos autónomos y la responsabilidad del fabricante, op. cit., p. 24.

portamiento individualizado a un modelo colectivo y sistematizado, en el que toda flota de vehículos autónomos será controlada y administrada por un único sistema operativo. En este escenario, se deberá realizar el cálculo de una prima de seguro del vehículo en base al riesgo que recaiga en el consumidor final¹¹⁴. De este modo, viene a sostener el autor que, debido a que el sistema operativo en funcionamiento ordenará a cada vehículo en circulación cómo comportarse, será el propio sistema el que cause el fallo, por lo que las circunstancias particulares que acontezcan en el accidente no tendrán sentido tomarlas en consideración¹¹⁵. Esta es la posición que también mantiene la doctrina más cercana al sector asegurador. Iturmendi señala que esta responsabilidad debe regularse ex novo al encontrarnos ante un marco jurídico actual que no puede contemplar este nuevo riesgo¹¹⁶.

Por su parte, el legislador europeo ha establecido que debe revisarse la Directiva del seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles a la luz de la evolución tecnológica y del incremento de uso de vehículos autónomos y semiautónomos¹¹⁷.

Aunque, ya hemos tenido ocasión de defender el sistema *no fault* de indemnización por daños causados por vehículos motor¹¹⁸, sobre la base de un seguro más próximo al de daños que al de responsabilidad civil, lo que no podemos mantener es su aplicación solo para los vehículos autónomos. Bajo esa premisa, cabe preguntarnos por qué razón una persona que sufre un accidente de circulación debe recibir una mayor o menor protección si utiliza un vehículo convencional o uno autónomo, pues obviamente la nece-

¹¹⁴ Geistfeld, M. A. (2017). A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, Vol 105, pp. 1621-1622 <https://ssrn.com/abstract=2931168>

¹¹⁵ Id. ib., pp. 1622-1623.

¹¹⁶ “Careciendo de conductor el vehículo autónomo comunicado, el legislador deberá regular ex novo la responsabilidad civil del dueño del vehículo, con independencia de dictar una normativa específica que regule la responsabilidad del fabricante del vehículo”. Iturmedi Morales, G. (2017). Coches autónomos y conectados. El papel de las aseguradoras. *Revista de la Asociación Española de Abogados especializados en Responsabilidad civil y seguros*, n° 61, p. 21.

¹¹⁷ Se ha dictado la Directiva (UE) 2021/2118 del Parlamento Europeo y del Consejo de 24 de noviembre de 2021 por la que se modifica la Directiva 2009/103/CE relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad, cuyo artículo 28 quater:2 establece que, a más tardar el 24 de diciembre de 2030, la Comisión presentará al Parlamento Europeo y al Consejo al Comité Económico y Social Europeo un informe de evaluación de la aplicación de la presente Directiva en lo que atañe a los avances tecnológicos, en particular en relación con los vehículos autónomos y semiautónomos; y de la adecuación del ámbito de aplicación de la presente Directiva, teniendo en cuenta los riesgos de accidente que comportan los distintos vehículos automóviles. Este irá acompañado, en su caso, de una propuesta legislativa.

¹¹⁸ Monterroso Casado, E. (2009). *Responsabilidad por accidentes de circulación. La concurrencia de causas*, Aranzadi, Navarra, pp, 510-525.

sidad de resarcimiento es la misma en ambos casos. Si se aboga por ese tipo de seguro debería ser para todos los casos, siendo estos costes repartidos, «pulverizados», entre todos los propietarios de vehículos, convencionales o autónomos, mediante el seguro obligatorio suscrito, que en definitiva es lo que se viene realizando con los seguros de responsabilidad civil por accidentes de circulación. Cuestión distinta es que las primas pudieran diferir en función del riesgo que entrañan unos y otros vehículos, cuyos propietarios deberían contribuir al sostenimiento de las primas necesarias para efectuar una completa cobertura de los daños ocasionados. En una primera fase, si tenemos en cuenta que el vehículo precisa del reconocimiento de infinidad de patrones (a pesar de los sandbox o entornos de prueba, el aprendizaje no será tan inmediato), junto al resto de factores implicados en el entorno operacional, las cifras de accidentes ocasionados y sus costes podrían no ser tan optimistas como se espera.

7. CONCLUSIONES

- Los cambios tecnológicos en la industria automovilística y la necesidad de protección a las víctimas de los accidentes van a ocasionar cambios importantes en el derecho de daños, aún de mayor envergadura de los que han ido sucediendo en las últimas décadas.
- Los sistemas avanzados de asistencia al conductor crean unas tareas de conducción dinámicas que permite que los automóviles puedan circular sin necesidad de la intervención humana. No obstante, aunque sea posible que esos sistemas realicen todas las tareas de conducción, prescindiendo del conductor, no se podrá aprobar un nivel de conducción de automatización alta (nivel 4) o completa (nivel 5) hasta que exista un entorno de IA con la infraestructura necesaria.
- La implantación del coche autónomo no es solo cuestión de una reforma legal que permita su autorización y puesta en circulación, sino que es preciso contar con un adecuado entorno operacional de uso definido, con una infraestructura en las carreteras y vías públicas donde se instalen sensores, cámaras y sistemas de comunicación, que posibilite una percepción y una interacción con ese entorno, que garantice el uso de esa tecnología disponible a la par que se dote de seguridad a los usuarios y donde también se vea garantizada la privacidad.

- La responsabilidad civil de los sistemas basados en IA debe regularse mediante legislación ad hoc. El RIA no prevé ninguna regulación específica sobre el régimen de responsabilidad civil de los sistemas de IA de alto riesgo, entre los que se incluirían los sistemas avanzados de asistencia al conductor (ADAS) que son los que, en gran medida, permiten la existencia de vehículos autónomos.
- La propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial no establece un régimen de responsabilidad, sino unos mecanismos para proteger a las víctimas, que deben aplicarse, sin perjuicio de las normas de los Estados miembros. Se trataría de una protección de mínimos y, por lo tanto, puede ser ampliada por nuestro ordenamiento.
- Se debe realizar una regulación específica de la conducción autónoma, con unas premisas que sean uniformes para todo el ordenamiento europeo, para evitar criterios de fragmentación jurídica entre los Estados miembros, siendo perentorio que se adopte esa legislación específica, como ya ocurre con los vehículos autónomos aéreos (drones).
- Al ir irrumpiendo en nuestras vías vehículos con distintos niveles de autonomía, el legislador tendrá que adaptarse a la convivencia de los mismos, incluso en una primera fase con una mayor presencia de vehículos convencionales. Se necesita una regulación europea unificada que proporcione seguridad jurídica, con cierto grado de armonización entre los Estados miembros y una garantía de que se proporcione una compensación adecuada para las víctimas con independencia del vehículo utilizado.
- Respecto a los requisitos de la conducción autónoma y las normas de circulación que, por su naturaleza, trascienden la normativa nacional actual de los vehículos convencionales, las propuestas de reforma del Reglamento Reglamento General de Circulación y del Reglamento General de Vehículos van a permitir un marco regulatorio avanzado, con respecto a otros Estados miembros, sobre conducción y vehículos automatizados. Tras su aprobación, se establecerán las condiciones y requisitos para la circulación de estos vehículos, las obligaciones derivadas de su puesta en circulación, así como las autorizaciones administrativas precisas para su circulación y los datos que deben constar en el registro de vehículos.
- Nuestro ordenamiento jurídico cuenta con una pormenorizada y eficiente normativa sobre la responsabilidad civil por los daños causa-

dos en accidentes de circulación, que es el resultado de la evolución de su régimen derivado de la necesidad de adaptación de las distintas directivas europeas del seguro del automóvil y del avance social hacia la protección de las víctimas. La implantación de los vehículos autónomos supone un paso más en esa evolución, que entiendo que se debe acometer con una reforma de la LRCSCVM. Esta postura no impide que cuando la presencia de los vehículos autónomos en nuestras vías sea la única y el nivel de autonomía de los vehículos sea alto o total, sea más oportuno un nuevo régimen jurídico que se adapte mejor a dicho escenario.

- Las víctimas de un accidente de circulación deberían poder recibir la misma protección, sin importar el tipo de vehículo implicado. Es por ello que los Estados miembros deberían realizar modificaciones en sus normativas específicas de circulación de vehículos para introducir normas particulares o ajustes, junto a las generales, que puedan resultar de aplicación a estos supuestos.
- Respecto al criterio de imputación de la responsabilidad en virtud del riesgo no parece que existan, en principio, inconvenientes para aplicar este criterio también en el caso de un vehículo de conducción autónoma que carezca de conductor. Aunque se haya comprobado que ese tipo de conducción sea más segura, no debería de dejar de considerarse como una actividad generadora de daños cubierta por el correspondiente seguro obligatorio.
- Entre las modificaciones precisas que deben abordarse en la LRCSCVM se encuentra extender la aplicación de este criterio de imputación de la responsabilidad en virtud del riesgo al operador en el caso de vehículos de conducción autónoma que carezcan de conductor, manteniendo la responsabilidad del propietario sin que sea precisa una relación de dependencia con el operador.
- Por otro lado, debería eliminarse de la LRCSCVM la diferente regulación entre daños materiales y corporales causados, y que existiera un único régimen de responsabilidad que evitase que el caso fortuito eximiera de responsabilidad, incluso en el supuesto de daños materiales.
- La reforma regulatoria no debería posibilitar que se incluyeran los productos defectuosos como causa de exoneración de la responsabilidad en la reparación del daño frente a la víctima. Por un lado, la opacidad y complejidad de estos sistemas basados en IA de alto riesgo dificultan poder determinar que la causa del daño sea el defecto

del sistema, aunque la propuesta de directiva de productos defectuosos incorpore, como sucede con la LIA, mecanismos de facilidad de prueba del nexo causal probabilístico. Por otro lado, la LRCSCVM otorga mayor protección a la víctima para que sea indemnizada debido a que el defecto del vehículo no se considera un supuesto de fuerza mayor extraña a la conducción capaz de exonerar de responsabilidad; sin perjuicio de que la aseguradora del vehículo pueda reclamar contra el fabricante por los defectos del mismo. Sería oportuno añadir que tampoco lo sería el fallo de aplicaciones y software. Cuestión distinta en que se quieran imponer ciertas obligaciones como la actualización del software y habilitar sanciones administrativas por su incumplimiento.

- Podría resultar análogamente de aplicación como contribución causal, la actual regulación relativa a los supuestos de ausencia de elementos o dispositivos de seguridad que pudieran provocar una agravación del daño, que podría incluso aplicarse a los casos en los que estos se hubieran desactivado, incumpliendo la normativa que dispusiera su uso obligatorio, y pudiera probarse que hubieran evitado o aminorado el daño.
- En los casos de daños personales por colisión recíproca sin determinación del grado o porcentaje de culpa de cada conductor en un escenario de conducción autónoma, el resultado debería ser el de la plena reparación de los daños causados al contrario con arreglo a la doctrina de las indemnizaciones cruzadas. En el caso de daños materiales, con la legislación actual, el conductor sería el que asumiera la indemnización de los daños del otro vehículo en un 50%, siendo deseable una reforma legislativa donde se acuda al criterio del resarcimiento cruzado de daños.
- Como el escenario actual del sistema de responsabilidad civil en el ámbito de la circulación de vehículos a motor ha quedado deformado, al incorporar a nuestro ordenamiento, un modelo de indemnización que no obedece claramente ni a un sistema de responsabilidad ni a un sistema de indemnización por daños, ello facilita que pueda también extenderse a la nueva realidad de circulación autónoma de vehículos donde el concepto de negligencia imputable a un sujeto concreto será en muchos casos imposible de determinar
- Debería aplicarse a los daños causados en los accidentes de circulación un sistema de indemnización sin culpa cubierto por el correspondiente seguro obligatorio, que debería configurarse más como un seguro cercano al de daños que como un seguro de responsa-

bilidad civil, tanto para vehículos convencionales como autónomos, siendo ese coste repartido entre los propietarios de los vehículo y sin que ello deba implicar inexorablemente asumir idénticas primas, sino que estarán en función del índice de siniestralidad o del riesgo que entrañan el uso de ese tipo de vehículo.

- Por todo ello, considero que no es preciso delimitar los tipos de responsabilidades en función de los niveles de automatización, sino aplicar un sistema uniforme de indemnización, sin perjuicio de las facultades de repetición contra terceros. No se trata de imputar la responsabilidad tomando como fundamento el deber de control sobre el vehículo autónomo (como sucede con otros robots), en el que además su propia autonomía podría imposibilitar la misma. Existen ya en nuestro ordenamiento unos mecanismos eficaces de protección a las víctimas de accidentes de circulación fruto de una necesidad social, que cuenta además con un seguro obligatorio (cuyas primas son abonadas por los propietarios de los vehículos) y que pueden ser ajustados, mediante las reformas oportunas, a la nueva realidad de los vehículos autónomos.

8. BIBLIOGRAFÍA

- Abraham, K, and Robert L. Rabin, R. (2019). Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era. *Virginia Law Review*, vol. 105, 2019, pp. 127-171.
- Álvarez Olalla, P. (2017). Desafíos legales ante la circulación de los coches autónomos: implicaciones éticas, responsabilidad por accidente y ciberseguridad. *Revista Doctrinal Aranzadi Civil-Mercantil*, n° 2, pp. 129-138.
- Álvarez Olalla, P. (2019). Responsabilidad civil en la circulación de vehículos autónomos. En E. Monterroso Casado (dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Tirant lo Blanch, Valencia, pp. 145-163.
- Álvarez Olalla, P. (2021). Propuesta de reglamento en materia de responsabilidad civil por el uso de Inteligencia Artificial, del Parlamento Europeo, de 20 de octubre, *Revista Cesco*, N° 38, pp. 1-10. doi.org/10.18239/RCDC_2021.38.2742
- Arcos Vieira, M. L. (2005). *Responsabilidad civil: nexos causal e imputación objetiva en la jurisprudencia*, Aranzadi, Pamplona.
- Atienza Navarro, M. L. (2023). ¿Una nueva responsabilidad por productos defectuosos?. Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28

- de septiembre de 2022 (COM/2022/495)". *InDret*, n.º 2, pp. 1-53. <https://doi.org/10.31009/InDret.2023.i2.01>
- Castells i Marqués, M. (2017). Vehículos autónomos y semautónomos. En S. Navas Navarro (coord.), *Inteligencia artificial, Tecnología, Derecho*, Tirant lo Blanch, Valencia, pp. 101-121.
- DGT (2024) *Vehículos de conducción automatizada*, 21 marzo 2024 <https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/vehiculos-de-conduccion-automatizada/>
- DGT (2024). Vehículos seguros y conectados. *Estrategia de Seguridad Vial 2030*, <https://seguridadvial2030.dgt.es/areas-estrategicas/vehiculos-seguros-y-conectados/>
- Díez-Picazo, L. (1999). *Derecho de Daños*, Civitas, Madrid.
- Doménech Pascual, G. (2019). Sobre el poder explicativo del análisis económico del Derecho. En especial, del Derecho de daños. *InDret*, n.º 2, pp. 1-39. <https://indret.com/wp-content/uploads/2019/07/1465-.pdf>
- Ebers, M. (2016). La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil? *InDret*, pp. 4-17. <https://raco.cat/index.php/InDret/article/view/314400/404514>.
- Eguiluz Castañeira, J. y Fernández Hernández, C. (2024). Diez puntos críticos del Reglamento europeo de Inteligencia Artificial", *La Ley*, 21 mayo 2024. <https://diariolaley.laleynext.es/dll/2024/06/28/diez-puntos-criticos-del-reglamento-europeo-de-inteligencia-artificial>
- Elizalde Salazar, I. (2022). *Vehículos autónomos. Responsabilidad civil y seguro*, Aranzadi, Navarra.
- Fernández Arévalo, A. y Murga Fernández, J.P. (2024). Civil Liability for Damage Caused by Autonomous Vehicles Under Spanish Law. En Hans Steege et al., *Autonomous Vehicles and Civil Liability in a Global Perspective*, Springer, 2024, pp. 345-359.
- Fernández Hernández, C. (2022). La Comisión presenta una propuesta de Directiva sobre responsabilidad civil extracontractual en materia de IA, *Diario La Ley*, N° 65, 29 de septiembre de 2022.
- Geistfeld, M. A. (2017). A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, Vol 105, 2017, pp. 1611-1694. <https://ssrn.com/abstract=2931168>
- Gil Membrado, C. (2024). Daños producidos por la IA: la opacidad del algoritmo y el efecto de caja negra. En Álvarez Lata, N. (Coord.) et al.: *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, pp. 501-547.
- Gómez Ligüerre, C. (2022). La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos. *InDret*, n.º 4, 2022. <https://indret.com/la-propuesta-de-directiva-sobre-responsabilidad-por-danos-causados-por-productos-defectuosos/>

- González Alonso, A. (2021). Responsabilidad civil y vehículos de conducción autónoma. ¿o no? En E. Llamas Pombo, J. Arrubla Paucar y C.I. Jaramillo (Dir.). *Derecho de daños y protección de la persona*, Tirant lo Blanch, Valencia, pp. 215-220.
- Iturmedi Morales, G. (2017). Coches autónomos y conectados. El papel de las aseguradoras, *Revista de la Asociación Española de Abogados especializados en Responsabilidad civil y seguros*, n.º 61, pp. 9-24.
- Izquierdo Grau, G. (2023). La responsabilidad del productor de vehículos autónomos en el marco de la (futura) legislación en materia de responsabilidad por daños causados por productos defectuosos. *Revista de Derecho Civil*, vol. X, núm. 2, pp. 117-161 <http://nreg.es/ojs/index.php/RDC>
- Kubica, M. L. (2022). Autonomous Vehicles and Liability Law. *The American Journal of Comparative Law*, Vol. 70, pp. 139-169, <https://doi.org/10.1093/ajcl/avac015>
- LeValley, D.. (2013). Autonomous Vehicle Liability—Application of Common Carrier Liability. *Seattle University Law Review*, Vol. 36, pp. 5-26. <https://core.ac.uk/download/pdf/235988125.pdf>
- López Mas, P.J. (2024). La responsabilidad civil en la conducción de vehículos autónomos o semiautónomos y su aseguramiento. *RCDI*, n.º 801, pp. 59-102.
- Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, n.º 4, pp. 1-9.
- Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, n.º 3, págs. 55-100. <https://doi.org/10.31009/InDret.2023.i3.02>
- Monterroso Casado E. (dir.) (2019), *Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento*, Tirant lo Blanch, Valencia.
- Monterroso Casado, E. (2009). *Responsabilidad por accidentes de circulación. La concurrencia de causas*, Aranzadi, Navarra.
- Monterroso Casado, E. (2019). Repercusiones de la inteligencia artificial en el ámbito de la responsabilidad civil. *Revista de responsabilidad civil, circulación y seguro*, n.º 11, pp. 6-20.
- Monterroso Casado, E. (2020). De la responsabilidad civil a la indemnización por daños derivados de la contribución causal al accidente de circulación. En López y García de la Serrana, J. (Dir.), *Responsabilidad civil y Seguro. Homenaje a Mariano Medina Crespo* Sepin, Madrid, pp. 813-848.
- Monterroso Casado, E. (2020). *Responsabilidad civil derivada de los accidentes de circulación y valoración de daños a las personas conforme a la Ley 35/2015, de 22 de septiembre*, CEF, 4ª ed., Madrid.
- Monterroso, Casado, E. (2020). Responsabilidad civil derivada de los daños en los bienes causados por colisión recíproca de vehículos. *RCDI*, 781, pp. 3188 a 3205.

- Monterroso Casado, E. (2022). Análisis de la imputación de la responsabilidad profesional en el nuevo escenario de la inteligencia artificial. En A. Muñoz Villareal (dir.), *Derecho de los Riesgos Tecnológicos*, EOLAS, Madrid, pp. 201-234.
- Monterroso Casado, E. (2024). *Robots and Liability: New Criteria and Attribution Methods*. En Moura Vicente, D., Soares Pereira, R., Alves Leal, A. (eds). *Legal Aspects of Autonomous Systems*. Springer, pp. 117-137.
- Muñoz Vela, J. M. (2023). IA y responsabilidad civil. Comentarios a las propuestas europeas en materia de derechos de daños por productos defectuosos y adaptación de las normas de responsabilidad civil extracontractual. *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 61. pp. 1-12.
- Navarro-Michel (2020) La aplicación de la normativa sobre accidentes de tráfico a los causados por vehículos automatizados y autónomos. *Cuadernos de Derecho Transnacional*, Vol. 12, n.º 1, pp. 941-961.
- Navarro-Michel, M. (2020). Vehículos automatizados y responsabilidad por producto. *Revista de Derecho Civil*, vol. VII, n.º 5, pp. 175- 223.
- Núñez Zorrilla, M.^a C. (2021). Los nuevos avances en la regulación europea de la responsabilidad civil por los daños ocasionados en el ámbito del transporte con inteligencia artificial. *Revista Europea de Derecho Europeo*, núm. 78-79, pp. 201–256. https://doi.org/10.37417/REDE/num78-79_2021_636
- Núñez Zorrilla, M.^a C. (2023). Hacia un marco legal europeo uniforme en la prevención de los riesgos y de la responsabilidad civil en el ámbito de la conducción automatizada inteligente”. *Cuadernos de Derecho Transnacional*, Vol. 15, n.º 1, pp. 689-723.
- Ortiz Fernández, M. (2024). La «adaptación» del derecho de daños a la inteligencia artificial: la propuesta de Directiva sobre responsabilidad. *IDP*, n.º 40, pp. 1-12, <https://raco.cat/index.php/IDP/article/view/n40-ortiz>.
- Pacheco Jiménez, M.^a N. (2024). Sistemas de inteligencia artificial para la toma automatizada de decisiones: algunos problemas de los contratos algorítmicos concluidos son asistente digital, *Cuadernos de Derecho Privado*, Vol. 4, n.º 9, pp. 140-171. <https://cdp.editorialbercal.es/index.php/cuadernos/article/view/65/58>
- Pearl, T. (2019). *Alternative Victim Compensation Schemes*. *William & Mary Law Review* Vol. 60, n.º 5, pp. 1827-1891. <https://wmlawreview.org/sites/default/files/Pearl.pdf>
- Rapaczynski, A., (2016). Driverless Cars and the Much Delayed Tort Law Revolution. *Columbia Law and Economics Working Paper* No. 540, pp. 1-36. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764686
- Reglero Campos, F. (2004). *Tratado de Responsabilidad Civil*, Aranzadi, Pamplona.
- Rodríguez de las Heras Ballell T. (2023). La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial. *La Ley mercantil*, n.º 103.

- Rosemadi, J. F., Khong, D. W. K., & Radhakrishna, G. (2022). Civil Liability of Autonomous Vehicles: A Review of Literature. *IIUM Law Journal*, núm. 30 (2), pp. 155–179.
- Seijo Bar, A. (2020). El coche autónomo: una aproximación a la responsabilidad civil en la era digital. En Ortega Burgos, E. (dir.), *Nuevas tecnologías*, Tirant lo Blanch, Valencia, pp. 369-390.
- Steege, H. et al. (2024). *Autonomous Vehicles and Civil Liability in a Global Perspective*, Springer,
- Tesone, R. (2024), El Reglamento de Inteligencia Artificial de la Unión Europea: “Un Reglamento para una Nueva Era”. Principales Aspectos y Obligaciones, *El derecho.com*, Lefebvre. 12 julio 2024. <https://elderecho.com/el-reglamento-de-inteligencia-artificial-de-union-europea-principales-aspectos-y-obligaciones>
- Torroba Díaz, J. (2019). Los vehículos autónomos y la responsabilidad del fabricante. *Revista de Responsabilidad Civil y seguro*, n.º 55, pp. 6- 30.
- Van Uytsel, S. (2021). Different Liability Regimes for Autonomous Vehicles: One Preferable Above the Other? En S. Van Uytsel, y D. Vasconcellos Vargas (Eds.) *Autonomous Vehicles*, Springer, 2021, pp. 67-92.
- Vestri G. (2024). La Unión Europea estrena el Reglamento de Inteligencia Artificial (RIA). *Diario La Ley*, n.º 10550.

Impresión 3D en el ámbito médico: problemática de la responsabilidad civil -y patrimonial- y sus incidencias digitales y de inteligencia artificial por las reformas de la Unión Europea¹

JUAN ANTONIO MORENO MARTÍNEZ

*Catedrático de Derecho Civil
Universidad de Alicante*

Sumario: 1. La fabricación aditiva o impresión 3D. Las iniciativas de la Unión Europea. 2. La bioimpresión 3D como específica impresión en la medicina. La responsabilidad civil -y patrimonial-: Régimen legal aplicable. 2.1. Consideraciones generales. 2.2. Incidencias de la consideración de la bioimpresión como producto sanitario: Evaluación de la conformidad. La responsabilidad patrimonial de la Agencia Española del medicamento y productos sanitarios (AEMPS) y su delimitación con respecto a los casos de responsabilidad patrimonial de la Administración sanitaria. 2.3. La responsabilidad civil en la bioimpresión. 2.3.1. Consideraciones previas. Directiva del Consejo de las Comunidades Europeas, de 25 de junio de 1985, y Reglamento del Parlamento Europeo y del Consejo de 5 de abril de 2017. Tratamiento de la problemática en ciertos derechos extranjeros: Francia, Alemania e Italia. 2.3.2. Problemática en el Derecho español. Repercusiones de las normativas europeas acerca de la

¹ Este trabajo se enmarca en el Proyecto I+D+i (Referencia: PID2020-116185GB-I00) del Ministerio de Ciencia e Innovación: “La irrupción de la inteligencia artificial en el Derecho de Daños y su adaptación a las nuevas tecnologías”, en calidad de co-investigador principal. Así mismo en el Proyecto I+D+i de Excelencia PROMETEO 2023 (Referencia CIPROM/2022/40) de la Conselleria de Educación, Universidades y Empleo de la Generalitat Valenciana: “La nueva era de los algoritmos y la inteligencia artificial y su tutela jurídica-privada en el marco de la Unión Europea”, en calidad de investigador principal.

bioimpresión como producto defectuoso y del uso de las nuevas tecnologías. Su explícita consideración.

1. LA FABRICACIÓN ADITIVA O IMPRESIÓN EN 3D: LAS INICIATIVAS DE LA UNIÓN EUROPEA

En la realidad actual, las llamadas técnicas de fabricación por adición o impresión 3D han extendido su ámbito de aplicación a una gran variedad de áreas científicas, tecnológicas e industriales. Sus orígenes se cifran en la década de 1960 experimentándose un rápido crecimiento en sectores como los de la ingeniería, arquitectura, aeronáutica, automoción y medicina. En este último sector, tal y como veremos, debido a las particularidades concurrentes en el ámbito de la salud, la técnica de la impresión 3D ha ido evolucionado en la denominada bioimpresión, parcela precisamente sobre la cual centraremos con posterioridad nuestro análisis.

En aras a contextualizar la referida parcela a estudio, debe constatarse, con carácter previo y desde una perspectiva general, que la fabricación por adición o impresión 3D² consiste, en síntesis, en la creación por ordenador de un modelo tridimensional que se utiliza como indicativo de actuación para la superposición sucesivas de capas de material, hasta llegar a la estructura perseguida³.

Se puede fácilmente constatar, a través de distintos estudios de orden técnico acerca de la impresión 3D, que es a partir de la primera década del presente siglo cuando se experimenta un claro auge de dicha tecnología, por su extensión también de su ámbito de aplicación.

Paralelamente se observa ya, desde un punto de vista jurídico, la preocupación que suscita la aplicación de dicha tecnología en ciertas vertientes, a los fines de formular posibles soluciones jurídicas a los efectos de pretender

² El término “fabricación aditiva” es el que se corresponde con el propio de la vertiente industrial (ASTM F2792), mientras que el referido a la “Impresión 3D” se refiere a la acepción utilizada coloquialmente.

³ Con carácter más descriptivo, desde un punto de vista técnico, afirma ORTIZ GIL, A. que “para crear un modelo 3D el primer paso es su diseño con un software de renderizado 3D (tipo CAD). El modelo se guarda en una estereolitografía (fichero STL). El software de la impresora reinterpreta la información del fichero STL y la transforma en secciones horizontales 2D que serán las que la impresora vaya imprimiendo de modo aditivo hasta formar el objeto 3D completo”. “Las impresoras 3D como herramientas científicas”. En *Encuentros Multidisciplinares. Observatori Astronomic de la Universitat de Valencia*, nº 61, p. 1.

https://repositorio.uam.es/bitstream/handle/10486/687514/EM_61_6.pdf?sequence=1&isAllowed=y

no paralizar dicho desarrollo tecnológico. En particular, ello se observa en los sectores jurídicos de la propiedad intelectual y de la responsabilidad civil, donde se apuntan ya, en el seno de la doctrina⁴, puntuales intervenciones legislativas.

El termómetro de las preocupaciones jurídicas acerca de la aplicación de dichas tecnologías se puede fácilmente apreciar a partir de dos iniciativas de la Comisión Europea, donde se puede constatar ya, además, según veremos, una clara interrelación entre las mismas. Sin duda, dichas iniciativas incentivarían los distintos estudios jurídicos que sobre la tecnología 3D fueron efectuándose en los países de nuestro entorno⁵.

La primera iniciativa en el seno de la Comunidad Europea -de menor alcance que la segunda- está protagonizada por el Dictamen del Comité Económico y Social Europeo sobre “Vivir mañana, La impresión en 3D: una herramienta para reforzar la economía europea” (dictamen de iniciativa)⁶.

Del texto que se incorpora, destacaríamos ciertos aspectos, que se formulan a modo de conclusiones, recomendaciones y observaciones -generales y específicas- y donde algunas de ellas, según veremos, encontrarán una clara co-

⁴ Así, LE GOFFIC, C.: “Impression 3D et responsabilité”, *Journal du Droit de la Santé et de l'Assurance-Maladie* (JDSAM) 2016/2, n° 14, pp. 17 ss. <https://shs.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance-maladie-2016-2-page-17?lang=fr>

⁵ Dentro de este contexto, entre otros, en el Derecho italiano, CAERAN, M.: *La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile*, University of Trento, The Trento Law and Technology Research Group Student Paper, n. 24, 2016, pp. 168 ss. https://www.academia.edu/23479298/LA_DIGITALIZZAZIONE_DEL_PRODOTTO_DIFETTOSO_STAMPA_3D_E_RESPONSABILITA_C3%80_CIVILE_MIRCO_CAERAN; VERMEULEN, N./ HADDON, G./ SEYMOUR, T./ FAULKNER-JONE, A./ SHU, W.: “3D Bioprint me: a socioethical view of bioprinting human organs and tissue”, 2017. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5827711/>. En el Derecho alemán, MEYER, B./ SCHREIBER, S./ SCHMAUDER, M./ HÖHN, K./ HILGERS, L.: “3-D-Druck und Produktsicherheit: Informationen für Hersteller und andere geschäftsmäßige Nutzer”, DOI: 10.21934/baua:fokus20181121.

<https://www.baua.de/DE/Angebote/Publikationen/Fokus/3-D-Druck-Produktsicherheit>
BAUER, H.K./ HELLER, M./ FINK, M./ MARESCHE, D./ GARTNER, J.: “Social and legal frame conditions for 3D (and) bioprinting in medicine”, *International Journal of Computerized Dentistry*, 2016, 19(4), pp. 293 ss; WIEBE, A.: *Immaterialgüterrechtliche Aspekte des 3D-Drucks und Haftungsfragen*, Universität Göttingen, 2018, https://www.grur.org/uploads/tx_meeting/Wiebe_02.pdf; GRAF WESTPHALEN, F.: “3D-Druck: Rechtliche Herausforderungen durch neue Technologien”, 2016, <https://www.fgvw.de/neues/archiv-2016/3d-druck-rechtliche-herausforderungen-durch-neue-technologien>; SHAHINIAN, D.: “Wer für 3D-gedruckte Bauteile haftet”, https://www.mittelstandswiki.de/wissen/Haftung_beim_3D-Druck/; En el Derecho francés, LE GOFFIC, C.: *Ibid.*, loc. cit.; GARANT-AUBRY, J./ LÉGER-RIOPEL, N.: “L'imprimante 3D et le domaine de la santé: enjeux juridiques et éthiques”, 2016.

<https://www.chairesante.ca/articles/2016/limprimante-3d-et-le-domaine-de-la-sante-en-jeux-juridiques-et-ethiques/>

⁶ DOC 332 de 8.10. 2015, p. 36.

rrespondencia con lo que ira aconteciendo en torno a la problemática de la tecnología a estudio.

Así, dentro del tratamiento que destina a conclusiones y recomendaciones, destacaría las afirmaciones concernientes a resaltar la creciente importancia de la “fabricación aditiva”, y que la identifica como el “proceso de unir materiales para fabricar objetos con datos de modelos 3D, normalmente superponiendo capas, a diferencia de los denominados, métodos de fabricación sustractivos”. A este respecto, se afirma que constituye una de las tecnologías esenciales que definirán en el futuro el nuevo enfoque de la fabricación de productos y cadenas de suministros, en tanto que provocarán un considerable aumento en el volumen de materiales para la fabricación, como mercados de suministros más competitivos⁷.

En lo concerniente a las observaciones que dicha iniciativa comunicaría efectúa sobre las consecuencias jurídicas que va a experimentar el progresivo crecimiento de la fabricación aditiva, las reconduce, en lo esencial, a tres sectores jurídicos⁸, invocando convenientes intervenciones legislativas a los efectos de no provocar la paralización en el avance de esta tecnología.

Así, se invoca en primer lugar la necesidad de nuevos procesos que permitan la certificación de la fabricación aditiva, así como técnicas de control de calidad tendentes a garantizar que las normas se respetan. Se considera esencial que todos los elementos de la tecnología de fabricación aditiva (por ejemplo, los materiales, los equipos y los procesos) se acomoden a previas exigencias legales, a los fines de garantizar piezas de calidad reproducibles.

Se aconseja asimismo, en segundo lugar, convenientes modificaciones y adaptaciones legislativas en torno a la protección de la propiedad intelectual ante las nuevas vicisitudes que plantea la fabricación aditiva⁹.

No menos importantes son las claras incidencias que se producen en la vertiente de la responsabilidad civil por los distintos sujetos intervinientes en estas tecnologías, sean diseñadores, fabricantes o distribuidores, al surgir -tal como se evidencia- las consecuentes dudas acerca de quién resulta responsable¹⁰.

⁷ Afirmaciones extraídas de las conclusiones y recomendaciones 1.1, 1.8, 2.2, 2.4 y 2.7.

⁸ Véanse a este respecto las observaciones específicas, contenidas en el apartado. 3.3.

⁹ Se constata la potencial y significativa incidencia en la propiedad intelectual: “Los objetos descritos en un archivo digital podrían ser mucho más fáciles de copiar, distribuir y piratear. Podría ocurrir lo mismo con el sector musical y cinematográfico, donde se desarrollan nuevos modelos de carácter no comercial...”.

¹⁰ Se advierte explícitamente que dicha cuestión, de indudable trascendencia, constituye “un asunto de indudable preocupación cada vez mayor para el sector de la fabricación aditiva, es-

La segunda iniciativa comunitaria, de mayor alcance, está representada por la Resolución del Parlamento Europeo, de 3 de julio de 2018, “sobre impresión tridimensional, un reto en el ámbito de los derechos de la propiedad intelectual y de la responsabilidad civil” (2017/2007 (INI))¹¹. La interrelación con la primera iniciativa resulta clara, pues entre los documentos de que se sirve el Parlamento Europeo para aprobar la presente Resolución, se cita explícitamente el ya referido Dictamen del Comité Económico y Social Europeo.

De la presente Resolución del Parlamento Europeo, que se presenta en perfecta sintonía con la primera iniciativa, si bien con mayor profundidad en la descripción de la problemática, destacaría los siguientes aspectos.

Así, se corrobora, en clara correspondencia con la iniciativa comunitaria anterior, el rápido crecimiento que viene experimentando la impresión 3D en distintos ámbitos tecnológicos y empresariales, atendiendo a las indudables ventajas que la propia Comisión Europea reconoce para el desarrollo, diseño y modernización de distintos productos.

Se constata que la mayoría de sectores científicos e industrias punteras ya utilizan dicha tecnología, al ir comprobándose a través de su empleo, las novedosas y trascendentes oportunidades que la misma ofrece. Se detiene en considerar, entre otros ámbitos donde ha encontrado una clara proyección, el de la medicina, aeronáutica, automoción, aeroespacial, electrodomésticos, construcción, investigación arqueológica, arquitectura, ingeniería mecánica, industria del ocio e incluso el sector del diseño.

Aun con todo, se aprecia que en algunos de los ámbitos mencionados que presentan una gran potencialidad, tales como el médico o el aeroespacial, la carencia de una mínima regulación legal ha provocado una clara limitación en la utilización de la impresión 3D.

Se traslada en la presente Resolución, de igual forma que sucedía con la primera iniciativa comunitaria, las inquietudes específicas que en el orden jurídico puede suscitar la impresión 3D en los ámbitos de la propiedad intelectual (derecho de autor, patentes, diseños, marcas e indicaciones geográficas) y de la responsabilidad civil. A este respecto, la referida Resolución del Parlamento, se detiene muy pormenorizadamente en detallar en los referidos ámbitos los problemas que pueden suscitarse, en aras a una futura cobertura legal.

pecialmente por la flexibilización, la individualización y el autodiseño puede llevarla a un terreno desconocido”.

¹¹ La génesis de la Resolución fue la presentación y aprobación de un Informe por Joëlle Bergeron, diputada francesa del grupo Europa de la libertad y la democracia directa, dirigido a establecer recomendaciones legislativas y reglamentarias sobre la impresión 3D.

Así en el ámbito de la propiedad intelectual, además de invocar la necesidad de reforzar la concienciación pública sobre la protección de la propiedad en el ámbito de la impresión 3D¹², precisa, con carácter particular, la necesidad de extremar la cautela en algunos asuntos, como el cifrado y la protección de los archivos, con la finalidad de intentar evitar “la descarga y reproducción ilegal de estos ficheros u objetos protegidos y la reproducción de objetos ilegales”.

De igual forma, se evidencia que el ámbito de la responsabilidad civil es otro de los sectores que requiere una concreta regulación legal. Se pone de manifiesto, a este respecto, que en la tecnología de impresión 3D, dado la multiplicidad de participantes y el complejo procedimiento de fabricación del producto, se pueden generar serias dificultades en aras a que la víctima pueda identificar al concreto responsable. En función de tales premisas, se solicita a la Comisión que defina las concretas responsabilidades de los distintos participantes en la elaboración de un objeto en 3D. A este respecto, se trae a colación, entre otros: al “creador y proveedor del programa informático, fabricante de la impresora 3D, fabricante del programa informático utilizado por la impresora 3D, proveedor de materias primas, impresor del objeto, o cualquier otro intermediario que participe en la realización concreta del objeto”.

Tras las consideraciones expuestas, importaría precisar, en aras a delimitar el objeto del presente trabajo, que es en el sector de la medicina donde la tecnología 3D, por sus singularidades y crecientes aplicaciones, ha venido presentando verdaderos usos innovadores crecientes y, además, de indudable trascendencia, pues inciden en la mejora de la salud humana.

Pues bien, a la traslación de dicha tecnología 3D al sector de la medicina, conocida como bioimpresión, se destina el objeto del presente estudio. En síntesis, tras la descripción de dicha innovación tecnológica, incluidas sus crecientes aplicaciones y beneficios -sin desconocer sus limitaciones- se pretende analizar, dados los distintos sujetos intervinientes en el proceso de conformación del producto acabado, susceptible de causar daños, las consiguientes determinaciones de responsabilidades civiles.

¹² Se puntualiza que “los expertos jurídicos consideran que la impresión 3D no ha alterado en lo fundamental los derechos de propiedad intelectual, el archivo creado puede considerarse una obra y que, llegado el caso deberá ser protegido como tal; que, a corto y a medio plazo, y para luchar contra la falsificación, el principal reto consiste en garantizar una participación más estrecha de los intermediarios profesionales en la protección de los derechos de autor”. Se señala, no obstante, la necesidad “de seguir investigándose las soluciones de carácter técnico insuficientemente desarrolladas hasta la fecha, como por ejemplo la creación de bases de datos de archivos cifrados y protegidos o el diseño de impresoras conectadas y equipadas con un sistema capaz de gestionar los derechos de propiedad intelectual, o incluso favoreciendo la cooperación entre los fabricantes y las plataformas para poner a disposición de los profesionales y los consumidores archivos fiables”.

Junto a tales singularidades, en aras a un conveniente diagnóstico, debe tenerse presente que las correspondientes unidades de impresión deben cumplimentar exigencias normativas previas de certificación y de control de calidad en su funcionamiento, dado que su inobservancia puede originar también daños. Asimismo, no debe desconocerse que, en muchos casos, tal y como veremos, el proceso de impresión se genera también por un ente público, o en el desarrollo de su propia actividad. Todo ello hace, en definitiva, que debamos, según los casos, traer a colación distintos derechos materiales y órdenes jurisdiccionales ante una misma tipología de daños.

En definitiva, se trata de analizar las actuales correspondientes coberturas legales de esta novedosa tecnología de la bioimpresión y, en su caso, las que pudieran aconsejar su inmediata activación por parte del legislador.

2. LA BIOIMPRESIÓN 3D COMO ESPECÍFICA IMPRESIÓN EN LA MEDICINA. LA RESPONSABILIDAD CIVIL -Y PATRIMONIAL-: RÉGIMEN LEGAL APLICABLE

2.1. CONSIDERACIONES GENERALES

Aunque puede revestir cierta complejidad la descripción técnica del desarrollo de la tecnología de la bioimpresión -pues además presenta variantes, en función de su concreta aplicación-, en lo esencial, puede caracterizarse como un proceso de cultivo de células vivas, biomateriales y factores de crecimiento para fabricar estructuras tridimensionales complejas, tendentes, entre otras aplicaciones médicas, a regenerar la función de un tejido u órgano, la creación de modelos anatómicos o de prótesis personalizadas¹³.

¹³ En el “Informe sobre Bioimpresión en la medicina del futuro”, Coordinado por Jorcano Noval, J.L., se contiene una clarificadora descripción del proceso. Así, determina en primer lugar, con carácter general, que la bioimpresión es un proceso que consta de tres fases: una fase inicial de pre-bioimpresión, la fase en la que se realiza la bioimpresión propiamente dicha y, por último, una fase de post-bioimpresión. A continuación procede a describir, con carácter más detallado, los concretos pasos del proceso: “la toma de imágenes y el diseño digital de un modelo tridimensional de los que se quiere reproducir; la elección de los materiales y células que se van a emplear como biotintas; y por último la bioimpresión de la estructura (...). En la fase de pre-bioimpresión resulta crucial la etapa de selección de las células (...). Las etapas de toma de imágenes y de diseño digital serán pasos esenciales de cara a generar órganos sólidos, ya que de ellos depende la capacidad para reproducir la arquitectura heterogénea y compleja de los mismos. En estas etapas, generalmente, se emplean tecnologías de imagen médica, como la Tomografía Computarizada y la Imagen por Resonancia Magnética (TIC e IRM) para proporcionar información precisa sobre la estructura tridimensional.

En el momento actual, entre las aplicaciones ya efectivas de la bioimpresión, convendría destacar las siguientes:

Desde los inicios de la articulación de la técnica de la bioimpresión, la aplicación más usual ha sido la de la generación de prótesis personalizadas o mejoras torácicas del paciente. A este respecto la prótesis de rodilla, fémur, o la reconstrucción de cadera, o maxilofaciales son prácticas médicas que se han venido presentando como potencialmente beneficiarias de esta técnica¹⁴. El transcurso del tiempo ha conllevado, en esta concreta aplicación, diseños más perfeccionados, dado que a partir de la mayor precisión de las imágenes que se obtienen del paciente y de los nuevos materiales que se incorporan (cerámicas, metales y polímeros) así como las estructuras que se conforman se consigue la máxima compatibilidad y personalización con el paciente.

Sin embargo, lo que debe destacarse en esta última década es el considerable aumento de aplicaciones de esta técnica, con los indudables efectos beneficiosos que ya está conllevando para la salud humana.

Así mismo, la bioimpresión 3D se está empleando frecuentemente como modelo preoperatorio en determinadas intervenciones quirúrgicas de cierta complejidad. Se consigue articular réplicas estructurales del paciente al objeto de poder planificar la concreta intervención quirúrgica. Sus efectos benefi-

En cuanto al modelo digital de la arquitectura de los tejidos, el diseño guiado por ordenador y fabricación guiada por ordenador (CAD y CAM) son las herramientas matemáticas empleadas con este fin". *Observatorio de Tendencias de medicina de precisión*, Fundación Instituto Roche, 2019, p. 14.

https://www.institutoroche.es/static/archivos/Informes_anticipando_BIOIMPRESION_digital.pdf

¹⁴ LOO GIL, C.: "Bio impresión 3 D: importancia en la actualidad", *TecnoHumanismo*. Revista Científica, febrero 2021, volumen 1/No.1.

<https://tecnohumanismo.online/index.php/tecnohumanismo/article/view/2>, pp. 99-101; ARANDA-BAULERO, M.: "Un cambio en los paradigmas de los sistemas de salud, la tecnología 3D", *Revista Peruana de investigación en Salud*, vol. 4, n. 3, 2020, pp. 121 ss.

<https://www.redalyc.org/journal/6357/635767700005/html/>; COUCKE, P.: "La médecine du futur. L'impression 3D en santé (1ère partie): Les structures à fonction non vitale", 2019, pp. 161-2. <https://orbi.uliege.be/bitstream/2268/268678/1/La%20m%C3%A9decine%20du%20futur%201%27impression%203D%20en%20sant%C3%A9%20les%20structures%20%C3%A0%20fonction%20non%20vitale.pdf>; KIRILLOVA, A./BUSHEV, A./ABUBAKIROV, A./SUKIKH, G.: "Bioethical and Legal Issues in 3D bioprinting", *International Journal of Bioprinting* (2020), v. 6, I. 3.

https://www.academia.edu/55980098/Bioethical_and_Legal_Issues_in_3D_Bioprinting pp. 7 ss; MENCACCI, M.: "Stampa 3D nel futuro della sanità: ecco gli usi pratici e i vantaggi", p. 4.

<https://www.agendadigitale.eu/sanita/stampa-3d-nel-futuro-della-sanita-ecco-gli-usi-pratici-e-i-vantaggi/>; TOMORROW BIO, "L'impatto delle protesi stampate in 3D sulla sanità moderna", <https://www.tomorrov.bio/it/post/l'impatto-delle-protesi-stampate-in-3d-sulla-sanità-moderna-2023-06-4727444136-3d-printing>

ciosos se han contrastado especialmente en cirugías craneofaciales¹⁵ y oncológicas¹⁶. Simular por anticipado todas las fases que indudablemente puede

¹⁵ Así CÉSAR-JUÁREZ, A.A./OLIVOS MEZÁ, A./LANDA SOLIS, C./CARDENAS-SORIA, V.H./SURIEL SILVA-BERMÚDEZ, P./SUAREZ ABEDO, C./OLIVOS DIAZ, B./IBARRA-PONCE DE LEÓN, J.C.: “Uso y aplicación de la tecnología de impresión y bioimpresión 3D en medicina”, *Revista de la Facultad de Medicina de la UNAM*, Vol. 61, n. 6, noviembre-diciembre 2018, p. 46.

https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0026-17422018000600043; YAN, Y./ XUEYAN, L./ GAO, Y./BHATTACHARYYA, A./ ZHAO, X./ ZHANG, S.C.: “3D bioprinting of human neural tissues with functional connectivity”, *TECNOLOGÍA*, V. 31, 2, [https://www.cell.com/cell-stem-cell/fulltext/S1934-5909\(23\)00439-3?_returnURL=https://linkinghub.elsevier.com/retrieve/pii/S1934590923004393](https://www.cell.com/cell-stem-cell/fulltext/S1934-5909(23)00439-3?_returnURL=https://linkinghub.elsevier.com/retrieve/pii/S1934590923004393).

Asimismo, en el marco de la realidad hospitalaria italiana, lo advierte VILLA, E., al permitir a los cirujanos analizar detenidamente, en relación a la corteza craneal y neuronal, las distintas opciones a partir de la patología existente, y todo ello con la finalidad de individualizar la cirugía más oportuna a practicar. “Stampa 3D in sanità: esempi e soluzioni per ospedali e strutture sanitarie”, pp. 6-7, <https://www.healthtech360.it/salute-digitale/stampa-3d-sanita-esempi-soluzioni/>

Recientemente, se ha tenido conocimiento de que un equipo de científicos de la Universidad de Wisconsin-Madison ha logrado crear un tejido cerebral humano funcional utilizando una técnica de bioimpresión 3D. En concreto, los investigadores imprimieron cultivos de corteza cerebral y estriado; dos tipos de tejido cerebral con funciones muy diferentes. A pesar de ello, los dos tejidos impresos en 3D lograron comunicarse entre sí. Estos avances tecnológicos abren la posibilidad de crear nuevas neuronas en cualquier momento, lo que podría servir para analizar cómo las partes sanas del cerebro interactúan con las partes afectadas por enfermedades, como por ejemplo el Alzheimer. Ver “Crean tejido cerebral humano funcional mediante bioimpresión 3D”, MCPRO, 7 febrero 2024.

<https://www.muycomputerpro.com/2024/02/07/cientificos-tejido-cerebral-humano-funcional-mediante-bioimpresion-3d#:~:text=Crean%20tejido%20cerebral%20humano%20funcional%20mediante%20bioimpresi%C3%B3n%203D,-Publicado%20el&text=Un%20equipo%20de%20cient%C3%ADficos%20de,una%20t%C3%A9cnica%20de%20bioimpresi%C3%B3n%203D>.

¹⁶ Dentro de este contexto, cabría traer a colación la reciente impresora 3D del Hospital 12 de Octubre de Madrid, que permite planificar cirugías complejas (fabricando moldes semejantes a los órganos que van a ser operados), y el tratamiento del cáncer con radioterapia, en sus dos facetas: radioterapia externa y braquiterapia. Dichas unidades de impresión 3D hospitalarias, que fabrican piezas en plena cirugía, han debido cumplimentar las exigencias normativas para su funcionamiento. En particular, se han observado, entre otras, las exigencias relativas a climatización y exposición a agentes químicos, ya que durante la fabricación se utilizan sustancias sintéticas, filamentos termoplásticos o disolventes. De igual forma, se obtuvo la Licencia de Fabricación de Productos Sanitarios. Finalmente se obtuvo la certificación conforme a la norma ISO de Aenor. Ver <https://www.abc.es/espana/madrid/impresora-hospital-octubre-fabricar-biomodelos-obtiene-certificacion-20240219022642-nt.html>

Asimismo, aunque situado en una fase más incipiente, cabría citar los avances llevados a cabo por un grupo de investigación de la Universidad de Granada (Cátedra de Investigación en células madre cancerígenas), en relación a la utilización de la bioimpresión 3D para desarrollar terapias personalizadas frente al melanoma maligno; el tipo más letal de cáncer de piel. “La relevancia de este estudio -se afirma- radica en la capacidad del modelo 3D bioimpreso para reproducir con precisión el microambiente tumoral del melanoma maligno, lo que nos facilitará estudiar con mayor detalle cómo interactúan las células tumorales con su entorno, y, lo más importante, es que se podrá identificar qué pacientes son más susceptibles o resistentes a un tratamiento determinado, permitiendo de este modo desarrollar tratamientos personalizados y más efectivos”. Con carácter más puntual, se detienen en describir el modelo creado, a partir de la réplica de la estructura de tres capas del melanoma maligno: “Para la capa superior se combinaron las células madre cancerígenas de melanoma

encontrar el facultativo utilizando modelos prototipos 3D puede contribuir a un mejor diagnóstico y planificación quirúrgica. Todo ello sin contar con la reducción de tiempos de cirugía y con ello los consiguientes riesgos que puede conllevar este tipo de intervenciones para el paciente¹⁷.

Otra de las posibles aplicaciones esperanzadoras de la bioimpresión, con la constatación ya de algunos resultados efectivos, se está produciendo en el ámbito de la investigación científica relacionada con la ingeniería de tejidos. Tal como se advierte en el seno de las aportaciones científicas, la tecnología de impresión 3D aplicada a la ingeniería de tejidos, se sustenta en la práctica de combinar, en lo esencial, células y moléculas biológicamente activas para crear tejidos funcionales¹⁸. En función de las estructuras biológicas que pueden conseguirse a través de la impresión 3D, estas se clasifican en cuatro niveles, que se hacen depender de la menor a mayor complejidad existente en su propia conformación. Así, estructuras sencillas, tal como la piel (nivel 1); estructuras tubulares huecas, como las de índole vascular (nivel 2); órganos huecos, que conllevan mayor complejidad, como vejigas (nivel 3); y por último, órganos sólidos, como el corazón, hígado o pulmones, donde la complejidad todavía es mucho mayor y por ello encontrándose esta técnica todavía en una fase muy incipiente, sin haberse llegado a materializar por el momento¹⁹. Se observa que la vascularización de los órganos,

maligno (de líneas celulares u obtenidas de pacientes) con queratinocitos humanos, mientras que en las capas intermedia e inferior se incorporaron fibroblastos, células endoteliales y células madre mesenquimales, todas ellas específicas del tejido nativo. Como material para simular la matriz extracelular del tumor se utilizó una composición basada en colágeno, el componente más abundante del tejido del melanoma". <https://catedracmc.ugr.es/bioimpresion-3d-modelo-melanoma-maligno/>.

¹⁷ CESAR JUÁREZ, A.A./Y OTROS.: *Op. cit.*, p. 46; ARANDA-BAULERO, M.: *Op. cit.*, pp. 3-4;

LEE, I.Y./SALAS-SÁNCHEZ, F./POMARES-WAUTERS, G./ RAMOS-GAMBOA, M.F./GODFREY-LOWIS, M./MORA-ROMÁN, J.J.: "Bioimpresión de órganos y tejidos en tercera dimensión: técnicas, aplicaciones y limitaciones", https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S0379-39822018000300041&lng=en&nrn=iso&tlng=es ; ZWETYENGA, N.: "L'impression 3D au service de la chirurgie", *Journal de Droit de la santé et de l'assurance maladie*, 2016, n° 14, <https://www.institutdroitsante.fr>, pp. 6 ss.

¹⁸ CESAR JUÁREZ, A.A./Y OTROS.: *Ibid.*, p. 46; "Informes anticipando bioimpresión en la medicina del futuro", Observatorio de tendencias de medicina personalizada de precisión. Fundación Instituto Roche (Coord. J. L. Jorcano Noval), *op. cit.*, p. 17; VERMEULEN, N./Y OTROS.: *Op. cit.*, p. 6; BISHOP, E.S./MOSTAFA, S./PAKVASA, M./LUU, H.H./ LEE, M.J./WOLF, J.M./AMEER, G.A./HE, T.C./REID, R.R., "3-D bioprinting technologies in tissue engineering and regenerative medicine: current and future trends", <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6003668>; JAIN, P./KATHURIA, H./DUBEY, N.: "Advances in 3D bioprinting of tissues/organs for regenerative medicine and in-vitro models", 2022, <https://www.sciencedirect.com/science/article/abs/pii/S0142961222002794>; WOLF, P.: "La bio-impression des avancées à petits pas", <https://lecardiologue.com/la-bio-impression-des-avancees-a-petit-pas/>

¹⁹ "Informes Bioimpresión en la medicina del futuro", (Coord. J. L. Jorcano Noval) *ibid.*, pp. 17-8.

por las inherentes dificultades del sistema de venas, arterias y capilares, revisite su principal obstáculo²⁰.

Dentro de las proyecciones descritas, solo en relación con los dos primeros niveles se han posibilitado ciertos éxitos en impresiones 3D. Así se constata, en particular, a través de investigaciones sobre la generación de piel, donde está llamada a conseguir resultados exitosos a corto plazo, sirviéndose del desarrollo creciente que está experimentando la utilización de esta tecnología, y con resultados de un indudable alcance más generalizado²¹. Ciertamente, la pretensión es la de abrir la posibilidad de imprimir piel en 3D directamente en el cuerpo, no faltando iniciativas investigadoras en este ámbito²², si bien

²⁰ En *TOMORROW BIO* se puntualiza que “Los vasos sanguíneos son esenciales para suministrar nutrientes y oxígeno a las células y eliminar los productos de desecho. Sin una red vascular funcional, los tejidos bioimpresos pueden no sobrevivir o funcionar correctamente. Los investigadores trabajan activamente en el desarrollo de estrategias para incorporar vasos sanguíneos a las estructuras bioimpresas, como el uso de materiales de sacrificio que puedan retirarse tras la impresión”, “Bioimpresión 3D: Un puente en los trasplantes de órganos”, 18-7-2023. <https://www.tomorrow.bio/es/post/la-bioimpresion-3d-como-puente-para-los-trasplantes-de-organos-2023-06-4727432548-3d-printing/>, p. 6; RICCOMANO, A.: “La stampa 3D al servizio della salute”, p. 3. <https://trendsanita.it/stampa-3d-salute/>

ZWETYENGA, N.: *Op. cit.*, pp. 6-7; GARCÍA GIL, M.: “Los retos que plantea la biotecnología al Derecho Privado. La Bioimpresión y el Bioderecho”, 2016, p. 28.

<https://repository.upb.edu.co/handle/20.500.11912/2774>; LOO GIL, C.: *Op. cit.*, p. 87; BAENA, J.M.: “Medicina regenerativa y bioimpresión 3D de tejidos y órganos”, <https://trepanos.es/2024/01/22/medicina-regenerativa-y-bioimpresion-3d-de-tejidos-y-organos>

²¹ CANTREAU, A.-S.: “Bioimpression: quelles responsabilités en cas de dommage”, <https://www.alain-bensoussan.com>, p. 2; *TOMORROW BIO*, *Ibid.*, p. 5; THIEULIN, C.: “Grâce à la bio-impression 3D, la greffe de peau est en pleine révolution”, 2024, <https://www.slate.fr/story/266037/bio-impression-3d-greffe-peau-traitement-brulures-medecine-recherche-technologie-revolution>; BOLGIANI, A./ HERMIDA, E.: “Bioimpresión 3D de piel”, *Cirugía plástica ibero-latinoamericana*, vol. 46, abril 2020,

https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0376-78922020000200014&lng=es&nrm=iso&tlng=es

Así, un grupo de investigadoras del IBEC, con sede en el Parque Científico de Barcelona, describen en la revista *Journal of Bioprinting* una nueva biotinta para sintetizar piel humana mediante la bioimpresión 3D, basada en luz visible, y utilizando nuevos hidrogeles. En síntesis, este estudio supone una nueva iniciativa para el desarrollo de nuevos tejidos cutáneos obtenidos con bioingeniería. Se considera que con dicho estudio se abre camino a la creación de complejos módulos *in vitro* de tejidos humanos. A este respecto CIRULLI, A./BORGHETTI-CARDOSO, L.N./TORRAS, N./MARTÍNEZ, E.: “Mimicking human skin constructs using nonporous pullulan-based hydrogels. *International Journal of Bioprinting* 3395. DOI: <https://doi.org/10.36922/ijb.3395>

Así mismo, en el marco de la Universidad de Leiden (Holanda) se consiguió unir dos tecnologías, la impresión 3D y el uso de células iPS creando células madre a partir de células ya diferenciadas y, dado que estas células se obtienen a partir de células del paciente, se consigue reducir las respuestas inmunes del paciente al tejido injertado. Se considera que es una técnica muy útil cuando se refiere a tratar heridas de gran tamaño. En García Gil, *op. cit.*, p. 30.

²² Así, en el marco de la Facultad de Medicina de la Universidad Wake Forest, se está desarrollando una impresora para fines militares, dirigida a imprimir piel directamente en pacientes que-

debe reconocerse que los largos periodos de tiempo que requiere esta cirugía la hacen inviable por el momento.

Otra de las aplicaciones que se perfila como de posible éxito a corto plazo es la utilización de la bioimpresión como técnica para generar medicamentos personalizados, y por ello haciéndose depender de las concretas deficiencias de salud que pudiera padecer el paciente²³. En función de tales premisas, se pretende diseñar comprimidos que contengan principios activos y niveles de dosis adecuadas en correspondencia con las características del paciente. Se persigue con ello mejorar la efectividad y reducir las posibles contraindicaciones²⁴.

2.2. INCIDENCIA DE LA CONSIDERACIÓN DE LA BIOIMPRESIÓN COMO PRODUCTO SANITARIO: EVALUACIÓN DE LA CONFORMIDAD. LA RESPONSABILIDAD PATRIMONIAL DE LA AGENCIA ESPAÑOLA DEL MEDICAMENTO Y PRODUCTOS SANITARIOS (AEMPS) Y SU DELIMITACIÓN CON RESPECTO A LOS CASOS DE RESPONSABILIDAD PATRIMONIAL DE LA ADMINISTRACIÓN SANITARIA

El proceso de la bioimpresión 3D, al posibilitar variados procesos de fabricación aditiva en aras a crear un objeto tangible, conlleva indudable dosis

mados. La “tinta” está fabricada con diferentes tipos de células epiteliales. <https://impresiontresde.com/cosas-impresion-3d-medica-puede-hacer-ya/>

Asimismo, en el marco español, cabe citar el equipo de científicos del Hospital Gregorio Marañón y Carlos III que ha presentado un prototipo de bioimpresión 3D capaz de crear piel humana funcional. Esta piel sería apta para ser trasplantada a pacientes, como para ser usada en investigación y pruebas de productos cosméticos, químicos y farmacéuticos. En la “tecnología de creación de piel (...) se utilizan jeringuillas con distintos componentes biológicos. La deposición de estas biotintas está controlada por ordenador y se realiza de manera ordenada en una placa para ir produciendo la piel. El proceso de bioimpresión de estos tejidos puede dar lugar (...) a la piel autóloga, creada de manera personalizada a partir de células de cada paciente, para usos terapéuticos como quemaduras graves”. Actualmente estas investigaciones están en fase de aprobación por diferentes entidades reguladoras europeas. “Primeros pasos de la impresión 3D de piel humana en España”. <https://www.institutoroche.es/noticiasmedicinapersonalizada/493>

²³ Todo ello, con independencia de que la impresión 3D haya sido ya utilizada como tecnología para crear un medicamento, sirviéndose de los controles administrativos pertinentes. Ello ha sucedido con el medicamento (píldora) Spritam levetiracetam, destinado a controlar las convulsiones provocadas por la epilepsia y comercializado por la compañía farmacéutica, con sede en Ohio. Se constató que la estructura de mayor porosidad que se consigue con esta tecnología provoca que se disuelva en contacto con el líquido, con mayor rapidez que la que resulta de la tableta convencional.

²⁴ “Informe Bioimpresión en la medicina del futuro”, (Coord. Jorcano Noval, J.L.), *op. cit.*, p. 10; VERMEULEN, N./ Y OTROS: *Op. cit.*, p. 6; ARANDA-BAULERO, M.: *Op. cit.*, p. 4. En el marco del Derecho italiano, VILLA, E., *op. cit.*, p. 9; RICCOMANO, A.: “La stampa 3D al servizio della salute”, <https://trendsanita.it/stampa-3d-salute>, pp. 2 y 4.

de complejidad a la hora de caracterizar unitariamente el propio proceso de conformación.

Aun con todo, tal como veremos, en función de las normativas que le serían aplicable, la fabricación aditiva 3D con finalidad médica se acomodaría, en propia caracterización, a la consideración de un producto sanitario, con las consecuencias que ello conlleva²⁵. Sirva de anticipo que dicha calificación legal de la bioimpresión se relacionará usualmente con el resultado de la articulación de los distintos componentes, si bien, en algunas ocasiones, alguno de sus elementos integrantes, podrá llegar a revestir autonomía al poseer propia caracterización, como podría ocurrir, tal como veremos, con el *software* con finalidad médica.

En aras a justificar las anteriores afirmaciones, y procurar, si cabe, una más correcta delimitación del supuesto a examen, convendría formular ciertas observaciones.

Así, en primer lugar, traer a colación, a nuestro entender, la fundamentación legal que le sería más propia. En efecto, el proceso de la bioimpresión 3D, a partir de noción amplia de “productos sanitarios” que proporciona el art. 2. del Reglamento (UE) 2017/747 del Parlamento Europeo y del Consejo de 5 de abril de 2017, encontraría en la misma el amparo normativo que le sería más acorde.

En particular, dentro de la anterior consideración se integran instrumentos, dispositivos, equipos informáticos, implantes, reactivos, así como cualquier “otro artículo destinado por el fabricante a ser utilizado en personas” con fines médicos específicos, ya sean de diagnóstico, de tratamiento o quirúrgicos²⁶. Así pues, el producto sanitario puede resultar, en función de la finalidad pretendida, a partir de la conformación de varios componentes o, tan solo por alguno de los mencionados, como usualmente se conforma el propio *programa informático*, siempre que el mismo, (como puntualiza el con-

²⁵ En este sentido ROBERT GUILLÉN, S.: “Marco regulador de la impresión y bio-impresión 3D para la aplicabilidad médica. Cuestiones sobre la patentabilidad de los productos de la bio-impresión 3D”. En *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 covid-19* (Susana Navas Navarro (dir.) Ed. Comares, p. 168.

²⁶ Se establece asimismo el condicionante de que no ejerza “su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos, ni metabólicos, pero a cuya función puedan contribuir tales mecanismos”.

Dicho amparo legal ya resultaba, si bien con descripción más sucinta, de la definición que de producto sanitario proporcionaba el art. 2.1) del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

siderando 19 del citado Reglamento) tenga una finalidad médica, ya sea de prevención, seguimiento, terapéutica u otra distinta²⁷.

A partir de tal caracterización, ello conllevará que el fabricante de la bioimpresión, a los efectos de que pueda estar disponible en relación con el usuario final, se someta a las exigencias de conformidad por parte del órgano administrativo que el propio Reglamento 2017/745 contempla²⁸. En nuestro país, tal como determina el art. 4.1. del R.D 193/2023, de 21 de marzo, por el que se regulan los productos sanitarios, es la Agencia Española de Medicamentos y productos sanitarios²⁹.

Debe precisarse a este último respecto que cuando se supera el procedimiento de evaluación de la conformidad previa del producto sanitario en cuestión³⁰, al ser observadas las distintas exigencias, se expide el certificado de conformidad, que posibilitará reflejar el marcado CE de conformidad del producto a los efectos de su comercialización.

Ahora bien, debe tenerse presente que en el proceso de conformación del objeto tangible en la bioimpresión suelen utilizarse materiales específicos que pueden conllevar sustancias peligrosas de distinto orden para la salud³¹.

²⁷ “Es necesario precisar que los programas informáticos por sí mismos, cuando están destinados específicamente por el fabricante a una o varias de las finalidades médicas establecidas en la definición de producto sanitario, son productos sanitarios, pero los programas informáticos para usos generales, aun cuando se utilicen en el marco de la asistencia sanitaria, o los programas informáticos destinados a objetivos de bienestar o estilo de vida, no son productos sanitarios. La calificación de programa informático, bien como producto sanitario o como un accesorio, es independiente de la ubicación del programa informático y del tipo de interconexión entre el programa informático y el producto”.

²⁸ En efecto, tras incluir la denominación “evaluación de conformidad”, entre las definiciones contenidas en el art. 2, (apartado 40) como identificativa “del proceso por el que se demuestra si un producto satisface los requisitos del presente Reglamento”, procede en su desarrollo normativo a perfilar el cumplimiento de tales exigencias. A este respecto, se destaca en su art. 19 la declaración de la UE de conformidad, donde constará que se ha cumplido en relación con el producto los requisitos específicos del presente Reglamento. Asimismo, en su art. 56 se aborda el periodo de validez de los certificados de conformidad, cuyo periodo será el especificado, sin que pudiera superar el plazo de cinco años.

²⁹ “La autoridad competente a la que se refiere el art. 101 del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, es la Agencia Española de Medicamentos y Productos sanitarios, independientemente de las competencias de otras autoridades sanitarias. La Agencia Española de Medicamentos y Productos Sanitarios decidirá sobre la aplicación a un producto de las definiciones y los criterios de clasificación de acuerdo con los arts. 2 y 51.2 y el anexo VII del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017”.

³⁰ A este respecto, de acuerdo a las previsiones contempladas en los Anexos IX, X y XI del Reglamento 2017/745, hay tres procedimientos distintos de evaluación de conformidad. Véase a este respecto el tratamiento efectuado por GARCÍA MICÓ, T. G., *La robótica quirúrgica y Derecho de Daños*, Marcial Pons, Madrid, 2024, pp. 54-58.

³¹ Así, a las bio-impresoras le será de aplicación la Directiva 2011/65/UE, de 8 de junio, sobre limitaciones al uso de determinadas sustancias peligrosas en aparatos eléctricos y electróni-

Ello determina que en el procedimiento de previa conformidad, y por ello antes de la disponibilidad del producto en el ámbito comercial, el organismo autorizante debe comprobar la acomodación de la bioimpresión -en función de la finalidad pretendida-, al marco legal que le sería de obligada observancia³². Ello no impide, además, cuando se trata de bioimpresión 3D, que los distintos fabricantes, en aras a mejorar las prácticas de la misma, se intenten acomodar a las normas internacionales incorporadas por la Organización Internacional de Normalización (ISO) y la Sociedad Estadounidense de Pruebas y Materiales (ASTM), pero a sabiendas de que, aun siendo normas de referencia en el sector, no revisten carácter obligatorio³³.

Téngase presente además que, en la propia definición de producto sanitario, se contienen nociones como “reactivos” (casos de filamento reactivos UV utilizados en la bioimpresión 3D) u otro “material u otro artículo destinado por el fabricante a ser utilizado en personas”, y por ello pueden llegar a tener la consideración de producto sanitario; si bien, usualmente, en su consideración de “producto intermedio”, o destinado a una “posterior transformación industrial por un fabricante autorizado”³⁴.

Resulta relevante destacar asimismo que la consideración de la bioimpresión 3D como producto sanitario, de acuerdo al Reglamento 2017/745, se hace depender de que el producto se encuentre “a disposición del usuario final como producto listo para ser utilizado en el mercado” (art. 2. 28 y 29)³⁵.

cos. De igual forma la Directiva 2012/19/UE, de 4 de julio, sobre residuos de aparatos eléctricos y electrónicos.

³² Así, deberá tenerse presente el art. 3.5 del RD 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios: “Los productos que sean máquinas de acuerdo con lo previsto en el Real Decreto 1644/2008, de 10 de octubre, por el que se establecen las normas para la comercialización y puesta en servicio de las máquinas, deberán cumplir asimismo los requisitos esenciales de seguridad y de salud previstos en el mismo, siempre que tales requisitos esenciales de seguridad y de salud sean más específicos que los requisitos generales de seguridad y funcionamiento previstos en el anexo I del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017.

³³ Las normas ISO y ASTM se confeccionan por consenso entre expertos y partes interesadas que representan diferentes perspectivas en la bioimpresión 3D. Dado que la bioimpresión es un ámbito en constante evolución, se van ofreciendo distintas instrucciones y normas. En lo esencial, dichas normas están referidas a materiales, donde se van describiendo los biomateriales estandarizados que sean compatibles y seguros con los procesos de bioimpresión; a estructuras celulares y tisulares; a imprimibilidad y resolución de estructuras complejas, etc.

³⁴ Esta última identificación se contiene en el art. 2 h) del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

³⁵ Dentro de este contexto, se cumplimentaría tales exigencias, cuando, con carácter puntual, se realizase una transferencia por el fabricante de un software, en su condición de producto sanitario (con independencia de su carácter oneroso o gratuito), al distribuidor, o al usuario final (en los casos de ser destinados a un hospital o centro de salud, estos tendrán dicha consideración). ROBERT GUILLÉN, S.: *Op. cit.*, p. 174.

Hasta ahora la bioimpresión 3D, se va reconduciendo, en cuanto a su caracterización, a su consideración de producto sanitario, con las consecuencias ya vistas. No obstante, en rigor, aunque ello sea lo que acontece en la gran mayoría de ocasiones, no por ello debe desconocerse que se producen ciertas bioimpresiones que escapan de las anteriores premisas.

Así, dentro de las aplicaciones de la bioimpresión, se consideró, en lo esencial, la tecnología de la impresión 3D, a partir de células y moléculas biológicamente activas del ser humano, y tendente a crear tejidos funcionales en el propio cuerpo humano. Pues bien, situándonos en un plano más general, el Reglamento 2017/745 determina, en su art. 2. 1. que quedarían fuera de la consideración de productos sanitarios, los productos que ejerzan su acción principal en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos o metabólicos. Con tales postulados, y relacionándolo con la noción que de “medicamento de uso humano” aporta el art. 2 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el Texto Refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios³⁶, se llega a la conclusión de que tales procesos de bioimpresión estarían relacionados más propiamente con la noción de medicamento, y no con la de un producto sanitario, en los casos en los que la acción principal de la bioimpresión, que se desarrolla en el cuerpo humano, pretenda fines farmacológicos, inmunológicos o metabólicos³⁷. Ciertamente, esta última bioimpresión, por su mayor alcance en la salud humana, y justificativa del seguimiento de exigencias, con carácter general más estrictas, no se separa mucho en relación con su consideración hipotética como producto sanitario, al hacerse depender su conformidad de la misma autoridad competente, es decir, de la Agencia Nacional de Medicamentos y Productos Sanitarios³⁸.

³⁶ “Toda sustancia o combinación de sustancias que se presente como poseedora de propiedades para el tratamiento o prevención de enfermedades en seres humanos o que pueda usarse en seres humanos o administrarse a seres humanos con el fin de restaurar, corregir o modificar las funciones fisiológicas ejerciendo una acción farmacológica, inmunológica o metabólica, o de establecer un diagnóstico médico”.

³⁷ No obstante, como advierte GALÁN CORTÉS, J.L, en caso de duda, cuando un producto sanitario pueda responder a la definición de medicamento, se le aplicará, de acuerdo al art. 8.6 del RD Legislativo 1/2015, de 24 de julio, el régimen de este último. Se produce, con ello, una *vis atractiva* del régimen del medicamento, dado que el mismo es más garantista y restrictivo, en virtud del principio general de primacía de la protección de la salud pública. *Responsabilidad civil médica*, Civitas, Cizur Menor (Navarra), 2022, p. 566.

³⁸ A este respecto se precisa que un producto fabricado mediante la tecnología de impresión 3D que incorpora células humanas viables como, por ejemplo, la impresión de tejido óseo con materiales biológicamente activos, tales como los “osteocitos”, tendrá la consideración de medicamento especial, en concreto, de “medicamento de terapia avanzada”, cuya regulación se encuentra en el Reglamento 1394/2007 de 13 de noviembre, sobre medicamentos de terapia avanzada, y que se encuentra además excluido de la consideración de producto sanitario por el art. 1.10 del Reglamento 2017/745. ROBERT GUILLÉN, *Op. cit.*, p. 177.

Así mismo podríamos encontrarnos con otras posibles variantes de bioimpresión, dentro de las aplicaciones que en su momento fueron descritas, que no llegasen a cumplimentar una finalidad médica consustancial a su caracterización general como producto sanitario. Dentro de tales postulados se presentarían aquellos productos creados con una finalidad estética³⁹. De igual forma, no verían cumplimentadas las exigencias de fin médico, aquellas bioimpresiones que atendieran a fines de investigación o educacionales⁴⁰. En consonancia con estos últimos postulados se encontrarían los modelos anatómicos utilizados en las distintas Facultades de Medicina.

A partir de lo ya descrito, cabría ya plantear una cuestión de relieve a nuestros efectos y es la de si, como consecuencia de los defectos que fueren imputables a la bioimpresión 3D, se generasen daños para sus destinatarios. A pesar de la complejidad que puede conllevar el proceso de bioimpresión, en función de las razones ya vistas, convendría formular, con carácter anticipado, ciertas precisiones que nos pudieran servir para clarificar el panorama acerca de los potenciales responsables.

Así, podría observarse que el defecto de la bioimpresión, causante de los citados daños, proviniese de una deficiente concepción de la bioimpresión y por ello pudiera verse cuestionada la “evaluación de conformidad”, otorgada por la Agencia Española del Medicamento y Productos Sanitarios (AEMS), sobre su puesta a disposición del público. A nuestro entender, no existiría ningún género de dudas acerca de que, si se verificase la falta de diligencia del referido órgano competente, de carácter público, en el otorgamiento de la referida conformidad, pudiera ser articulada, por los perjudicados afectados, la correspondiente responsabilidad patrimonial de la Administración⁴¹. Acerca de las anteriores afirmaciones convendría realizar ciertas matizaciones.

En primer lugar, situándonos en esa fase de control previo del producto, la potencial responsabilidad de la Administración podría verse extendida, en ciertos casos, al fabricante del producto resultante. En aras a justificar esta última responsabilidad, pensemos en ciertas tipologías de productos sanita-

³⁹ El Anexo XVI del Reglamento 2017/745 excluye explícitamente a “las lentes de contacto u otros artículos destinados a ser introducidos o colocados en el ojo”, Así mismo “los productos destinados a ser total o parcialmente introducidos en el cuerpo humano mediante medios invasivos de tipo quirúrgico a efectos de modificación de la anatomía o fijación de partes del cuerpo”.

⁴⁰ Aun con todo, puede revestir la consideración de “accesorio de un producto sanitario” cuando las bio-impresiones 3D fueran destinadas por su fabricante (de acuerdo al art. 2.2. del Reglamento 2017/745), de forma conjunta junto a otro producto sanitario con la finalidad de “permitir específicamente que este pueda utilizarse con arreglo a su finalidad prevista o para contribuir específica y directamente a la funcionalidad médica de los productos sanitarios a efectos de su finalidad prevista”.

⁴¹ Véase a este respecto ÁLVAREZ OLALLA, P.: “Daños causados al paciente por utilización de un producto sanitario defectuoso. Al hilo del caso Ala Octa”, *RCDI*, 2022, n° 794, pp. 3396-7.

rios donde el proceso de conformidad se valida, y se obtiene el sello de la UE a partir de una declaración del fabricante⁴², sin contar con el expediente presentado por el fabricante, que pudiera contener además certificaciones incompletas e inexactas. En tales casos hipotéticos de codemanda ante la jurisdicción contenciosa, única competente, la responsabilidad del fabricante final del producto podría ampararse de acuerdo al art. 133 TRLGDCU y sustanciarse procesalmente según lo dispuesto en el art. 9.4 LOPJ y 2 e) LJCA. Ello no significa que el perjudicado decida canalizar la demanda exclusivamente contra la Administración, en tanto que órgano competente para otorgar la “evaluación de conformidad”.

Así mismo estimamos, pese al certificado de conformidad de la Administración, que esta no debería verse responsabilizada cuando se comprobara que el defecto causante del daño obedecía a una tecnología en la que, en el momento de efectuar la “evaluación de conformidad”, se desconocía su efecto perjudicial.

A idénticas consecuencias exoneratorias para la Administración debiera llegarse cuando en el proceso de “evaluación de conformidad” por la misma, esta hubiera sido consciente, en su correspondiente diagnóstico, de los efectos perjudiciales del producto resultante, aunque también de sus indudables efectos beneficiosos y, posteriormente se llegase a determinar que los defectos procedentes de los primeros efectos fueron los causantes de los daños a los usuarios o pacientes. Así pues, como se ha constatado en la doctrina, en ese equilibrio del binomio beneficio-riesgo puede sustentarse una clara exoneración de la Administración⁴³.

En segundo lugar, debe precisarse que dicha responsabilidad, con carácter previo de la Administración, es perfectamente deslindable de la responsabilidad patrimonial de la Administración que, ya en la fase de aplicación del producto resultante de la bioimpresión 3D, pudiera ocasionarse al usuario o paciente, por su carácter defectuoso, y sin que la certificación de conformidad del producto sirviera de argumento para convalidar el defecto que pueda adolecer tras su comercialización⁴⁴.

Situándonos dentro de este último contexto, junto a las causas propiamente atribuibles a defectos funcionales del servicio público⁴⁵, como defectos

⁴² A este respecto véase, en cuanto a los productos sanitarios de la clase I, lo dispuesto en el art. 52.7 Reglamento 2017/745.

⁴³ En este sentido GRIMALT SERVERA, P.G.: “La responsabilidad (civil o patrimonial) del personal médico de los centros sanitarios y de las administraciones sanitarias por los daños causados por un producto sanitario defectuoso”, *Bioderecho.es*, núm. 17, enero-julio 2023, pp. 15-6. file:///C:/Users/Usuario/Downloads/Responsabilidad+por+productos+sanitarios+defectuosos.pdf.

⁴⁴ En este sentido GARCÍA-MICÓ, T.G.: *Op. cit.*, p. 121.

⁴⁵ En este sentido GRIMALT SERVERA, P.: *Op. cit.*, p. 11.

de mantenimiento de los materiales de la propia bio-impresora, habría que traer a colación los casos más usuales donde se observara que la causa atribuible de los daños descansa en una infracción de la *lex artis* de los facultativos, en su concepción de obligación de medios y, por ello, no de resultado. Así, como supuesto particular, podría traerse a colación el caso hipotético en el que se observara que la deficiente aplicación de la bioimpresión, al ser planificada por dicho medio, se hizo con grandes imprecisiones (en imágenes, por ejemplo) provocando que la intervención quirúrgica oncológica proyectada se viera dilatada en su desarrollo, y determinara como consecuencia la causación de ciertos daños sobrevenidos. De igual forma que en el caso anterior, podrían resultar codemandados en la jurisdicción contenciosa, al amparo de las referidas previsiones procesales, tanto la Administración como el fabricante de la bioimpresión.

2.3. RESPONSABILIDAD CIVIL EN LA BIOIMPRESIÓN

2.3.1. Consideraciones previas: Directiva del Consejo de la Comunidades Europeas, de 25 de junio de 1985 y Reglamento del Parlamento Europeo y del Consejo de 5 de abril de 2017. Tratamiento de la problemática en ciertos derechos extranjeros: Francia, Alemania e Italia

Procedería ya a continuación centrar nuestro interés en analizar el panorama de la responsabilidad civil por producto defectuoso resultante de un proceso de bioimpresión 3D. Ello conlleva que su proyección y problemática esté relacionada con el funcionamiento que se viene realizando por entes privados u hospitales privados. Ciertamente sus normas sustantivas o materiales aplicables se verán alteradas respecto a si el proceso de fabricación de la bioimpresión causante de los daños, según vimos con anterioridad, se hubiera desarrollado en el ámbito de un servicio sanitario público y donde el proceso de reclamación de los correspondientes daños debía canalizarse por el orden jurisdiccional contencioso. Ahora bien, ello no significaba que en ciertas hipótesis, tal como ya fue afirmado, determinadas previsiones legislativas, de naturaleza civil, pueden encontrar en la jurisdicción contenciosa perfecta justificación, y ello sucedería, en lo fundamental, según vimos, cuando junto a la Administración se codemandase al fabricante de la bioimpresión, encontrando, en consecuencia, aquellas previsiones un orden jurisdiccional que no es, en principio, el propio. Es por ello que el régimen legal aplicable a la responsabilidad por daños consecuencia de la bioimpresión presenta cierto rasgo de transversalidad.

Desde una perspectiva general, y antes de situar el termómetro en ciertos países de nuestro entorno, previo a fijarlo en nuestro derecho, convendría resaltar las características singulares que acompañan al fenómeno novedoso de la bioimpresión (en su conformación y sujetos intervinientes), y que, por su consideración, en lo esencial, de producto sanitario, se ha podido ya revestir de una especial tutela legal, en relación a los daños que pudieran ser generados por su carácter defectuoso.

En efecto, debemos traer a colación, por una parte, el referido Reglamento 2017/745 y, por otra, la Directiva del Consejo, de 25 de julio de 1985, en materia de responsabilidad por los daños causados por productos defectuosos. A nuestro entender, esta última normativa comunitaria, a nuestros efectos, no puede desconectarse de las previsiones normativas contenidas en el referido Reglamento, no solo por su aplicación directa, sino por acomodarse más a la actual realidad social en los extremos aquí analizados.

Las dificultades de cobertura legal, que en lo esencial y con distintas intensidades según los Derechos, vienen presentando los productos digitales en el concepto de producto del art. 2 de la Directiva 85/374, no resultan tales al amparo del art. 2 del Referido Reglamento. Debe tenerse presente que, según la propia Directiva, el producto sanitario no es más que una tipología de producto, y como tal consideración no debe ofrecer duda acerca de que la determinación del alcance de aquél debe corresponder más propiamente con lo previsto en su normativa específica, sin contar, como ya se ha dicho, con que la misma se presenta más acorde con la realidad que acompaña al proceso de la bioimpresión.

Pensemos a este respecto en la previsión que, acerca del “programa informático” incorpora en particular el art. 2 del Reglamento 2017/745, dentro de los componentes potenciales del concepto de producto sanitario, si bien sin desconocer las afirmaciones contenidas en su considerando 19, en el sentido de que el referido “programa informático” puede dejar de revestir la consideración del carácter accesorio, y por ello susceptible de constituir un producto independiente cuando el mismo esté destinado a una o varias finalidades médicas establecidas del referido art 2, sin que sea relevante su ubicación y el tipo de interconexión entre el programa informático y el producto⁴⁶. Así mismo,

⁴⁶ Dentro de este contexto se precisa que “si el software está destinado por su fabricante a ser usado “de forma conjunta”, según reza el mencionado art. 2.2, con una impresora 3D calificada como producto sanitario, para permitir que aquella pueda utilizarse con arreglo a su finalidad prevista o para contribuir específica y directamente a la funcionalidad médica de los productos sanitarios a efectos de su finalidad prevista, el software puede calificarse de accesorio de un producto sanitario. Conclusión que no es aplicable al software de diseño que se utiliza en una impresora 3D de uso general, y en la que se fabrican productos sanitarios, pues el hecho de que se imprima un producto sanitario y el software sirva como medio de fabricación aditiva, no está utilizando de forma conjunta

fiel testimonio de la actualidad de tal regulación (tal como se corroborará con posterioridad), son las propias previsiones que en el art. 23.2 se recogen acerca de la posibilidad de que puedan operarse modificaciones de las partes integrantes o de los componentes del producto sanitario, con la determinación de que, si revisten la consideración de cambios sustanciales, puedan erigirse ya en producto independiente, con las incidencias que ello conlleva en los potenciales responsables⁴⁷. Sin duda, estas distintas precisiones normativas que nos aporta el Reglamento 2017/745, son gran utilidad en su traslación al proceso de la bioimpresión y por ello deberán ser tenidas en cuenta en la determinación del alcance de los concretos ámbitos competenciales, y consecuentemente en la determinación de los potenciales responsables de los daños que se originen por los defectos del producto sanitario.

Tras estas consideraciones previas, destinadas a la caracterización general de la tutela legal de la bioimpresión, convendría detenernos en el tratamiento que en particular se ha venido otorgando por ciertos Derechos de nuestro entorno. Dentro de este contexto, debe ocupar un lugar destacado la relevancia que ya reviste en la atención médica hospitalaria francesa la presencia de la tecnología de impresión 3D -en sus distintas aplicaciones-, en aras, como así se advierte en el seno de distintos medios de difusión⁴⁸, de la búsqueda de una mayor eficiencia, precisión y seguridad de sus servicios médicos. Se invoca incluso, como deseable, una mayor extensión de las instalaciones de plataformas de impresión hasta la generalidad de los distintos hospitales existentes, aun siendo conscientes del gran aumento de recursos financieros que ello necesariamente conlleva, junto a la necesidad de una mayor capacitación del personal médico en aras a su manejo.

Paralelamente, se observa en la doctrina francesa un especial interés por la problemática jurídica que se genera con la incorporación de dicha tecnología de la bioimpresión en la práctica médica de los hospitales⁴⁹.

con el producto sanitario que se fabrica, y no puede ser calificado de accesorio del mismo". ROBERT GUILLÉN, R.: *Op. cit.*, pp. 173-4.

⁴⁷ "Un elemento destinado específicamente a sustituir una parte o un componente de un producto que modifique significativamente su funcionamiento o sus características de seguridad, o su finalidad prevista, se considerará un producto y cumplirá los requisitos establecidos en el presente Reglamento".

⁴⁸ <https://www.a3dm-magazine.fr/les-hopitaux-francais-adoptent-limpression-3d-pour-ameliorer-les-soins-medicaux/>

⁴⁹ Así, entre otros, LE GOFFIC, C.: *Op. cit.*, pp. 17 ss.; CANTREAU, A.-S.: *Op. cit.*, pp. 1 ss. <https://www.alain-bensoussan.com> ; MONTMARTÍN, M./MEYER, C./PAZART, L.: "L'impression 3D à l'hôpital: Quelle réglementation en France", *Revue de Stomatologie, de Chirurgie Maxillo-Faciale et de Chirurgie Orale*, V. 116, n.5, 2015, pp. 302 ss.

<https://www.sciencedirect.com/science/article/pii/S2213653315000737>; ZWETYENGA, N., *op. cit.*, p. 6 ss.

Indudablemente, la presencia de distintos componentes que se integran en la impresión resultante conlleva, en función de su concepción de accesoriadad, o autonomía de los mismos, indudables problemas de determinación de sus potenciales responsables, ante los posibles daños que genere la impresión defectuosa. Así, entre otras hipotéticas responsabilidades que pudieran generarse, se especifican las que pudieran ser atribuidas al diseñador del software asistido por ordenador; al creador del archivo CAD que se utilizará para imprimir el objeto; al proveedor del archivo CAD; al fabricante del objeto, en calidad de quien imprime físicamente el producto; o la que pudiera ser atribuida a los proveedores de materiales de impresión 3D.⁵⁰

Se ofrece, como pilar fundamental de apoyatura legal para resolver dicha problemática, la regulación incorporada en los arts. 1245-1245-17 y ss del Código Civil, acerca de la responsabilidad por productos defectuosos, tras su modificación por la Orden n.º 2016-131 de 10 de febrero de 2016. Dicha regulación supuso la correspondiente transposición, en el Derecho Francés, de la Directiva 85/374.

Ciertamente, el texto normativo acerca del concepto de producto defectuoso, contenido en el art. 1245-2⁵¹ no dista mucho del que se ofrece en el marco de otros Derechos extranjeros como resultado también de la transposición de la referida normativa comunitaria. Sin embargo, en el seno de la doctrina francesa, como claro signo distintivo, no ha habido reparos en flexibilizar la noción de producto y con ello las previsiones del Código Civil sobre bienes intangibles a la impresión 3D, como en los casos en particular, por ejemplo, en los que el software o los archivos CAD resultasen defectuosos.

En el seno de la doctrina, se trae a colación la cuestión controvertida acerca de si a través de la bioimpresión puede llevarse a cabo también en actos médicos no terapéuticos, con fines de aumentar artificialmente las capacidades o habilidades humanas. Se sabe ya en nuestros días que en el campo de la nanomedicina se pueden implantar directamente diferentes dispositivos en el cuerpo humano para aumentar sus capacidades (implantes protésicos en la corteza cerebral; chips artificiales para mejorar la memoria, etc.), y con ello con fines transhumanistas. A este respecto, se advierte de las divisiones existentes entre los especialistas, sustentadas en las innegables cuestiones éticas inherentes. A este respecto, LEQUILLERIER, C.: "Impression 3D et santé: Le possible interventionnisme du droit face au transhumanisme", *Journal de Droit de la santé et de l'assurance maladie*/2016, n. 14. <https://shs.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance-maladie-2016-2-page-12?lang=fr>; DEKEUWER-DEFOSSEZ, F.: "Réflexions sur l'acte médical non thérapeutique", in *Mélanges en l'honneur de Gérard Mémeteau, Droit médical et éthique médicale: regards contemporains*. Sous la dir. de J. Leonhard, B.P et F. Vialla, Vol. 1, 2015, pp. 399 ss.; PARICARD, S.: "Consentement aux actes médicaux non thérapeutiques", in *Consentement et santé*. Sous la dir. de l'Association française de droit de la santé, Dalloz, 2014, pp. 103 et ss.

⁵⁰ LE GOFFIC, C.; *Op. cit.*, pp. 17-8.

⁵¹ "Es un producto cualquier bien mueble, incluso si está incorporado a un inmueble, incluidos los productos de la tierra, la ganadería, la caza y la pesca. La electricidad se considera un producto".

En lo fundamental, se considera por la doctrina que, si en el concepto legal de producto se integra ya el bien intangible de la electricidad, no debe existir inconveniente para que dicha noción se vea extendida, por razones análogas a otros productos intangibles, según la actual realidad social⁵².

No obstante, no se desconoce tampoco por la doctrina que, en el ámbito a estudio, la víctima puede encontrarse en serias dificultades para acreditar el carácter defectuoso del producto. En su correspondiente acreditación deberá acudir a los criterios recogidos en el art. 1245-3⁵³ que no dejan de ser, en lo esencial, una clara transcripción de lo previsto por la Directiva 85/374.

A este respecto se aprecia que el carácter defectuoso puede resultar fácilmente de la estimación de la anomalía o imperfección en una serie concreta de un producto. Dentro de dicho contexto se cita, en la doctrina, como posible exponente ilustrativo, la sentencia del Tribunal de Justicia de la Unión Europea de 5 de marzo de 2015⁵⁴, donde, suponiendo que se utilizara una impresora 3 D para imprimir una serie de dispositivos médicos, “la demostración de un posible defecto en productos pertenecientes al mismo grupo o serie de producción, como marcapasos y desfibriladores automáticos implantables, resulta suficiente para calificar tal producto como defectuoso, sin que sea necesario constatar la existencia de dicho defecto en su generalidad”. Todo ello sin contar, tal como lo hace el Tribunal, con las exigencias de mayor seguridad, por la tipología de productos en cuestión (marcapasos cardíacos y los desfibriladores automáticos implantados), que los pacientes debían legítimamente esperar. Estas distintas circunstancias vienen a facilitar en gran medida la demostración por el demandante del defecto del producto y, en su caso, lo impreso en 3D.

Además, ya en relación con los daños reparables, el Tribunal apreció que los mismos debían extenderse, si fuera necesario, a los daños de índole corporal que se le causaren por la operación quirúrgica dirigida a sustituir el producto defectuoso. Como resultado de ello, tal como se advierte en la doctrina, si a los pacientes que se les hubiera implantado dispositivos médicos impresos 3D defectuosos, podrían obtener una compensación por los daños resultantes de la operación necesaria para extraer los referidos dispositivos⁵⁵.

⁵² CANTREAU, A-S.: *Op. cit.*, pp. 2-3; LE GOFFIC, C., *Op. cit.*, p. 18.

⁵³ “Un producto es defectuoso en el sentido de este capítulo cuando no ofrece la seguridad que legítimamente puede esperarse. A la hora de evaluar la seguridad que legítimamente cabe esperar, deberán tenerse en cuenta todas las circunstancias y, en particular, la presentación del producto, el uso que razonablemente cabe esperar del mismo y el momento de su utilización. Un producto no puede considerarse defectuoso simplemente porque posteriormente se puso en circulación otro más avanzado”.

⁵⁴ CJUE, 5 marzo 2015, *aff. jointes* C-505/13 et C-504/13, Boston Scientific, D. 2015, p. 1247, *obs.* J.-S. Borghetti. Citado por LE GOFFIC, C.: *Op. cit.*, p. 18.

⁵⁵ *Ibid.*, *loc. cit.*

Del resto de normativa reguladora de la responsabilidad por productos defectuosos, trasladable con las debidas adaptaciones a la impresión 3D, destacaríamos las previsiones en relación con la hipótesis de que el daño causado lo fuere por el defecto de un producto incorporado a otro, en cuyo caso se generaría una responsabilidad solidaria del productor del componente y de la persona que realizó la incorporación (art. 1245-7 CC). No obstante, según se contempla en el art. 1245-10, el productor del componente incorporado no respondería si demostrara que el defecto resultase atribuible al diseño del producto en el que se incorporó, o al seguimiento de las instrucciones otorgadas por el productor de este producto.

El segundo pilar regulador del Derecho francés en relación con la bioimpresión puede encontrar su justificación en los casos en los que el daño causado al paciente por el producto defectuoso se generase en el marco de los servicios hospitalarios, en calidad de prestatarios, al ser materializado por sus facultativos, y por ello el efecto dañino no se hubiese producido en calidad de fabricante del producto, donde, como se ya se ha visto, resultaría aplicable la anterior normativa del CC, resultado de la transposición de la referida Directiva 85/374.

Sobre este segundo pilar legal, debe acudir al art. L.1142.1, I, párrafo 1 del Código de Salud Pública, donde se aborda la posible responsabilidad médica para los casos en los que un producto sanitario defectuoso ocasione un daño⁵⁶.

Se advierte a este último respecto en el seno de la doctrina⁵⁷ que, aun cuando exista coincidencia, tanto por el Tribunal de Casación como por el Consejo de Estado, acerca de la potencialidad de la responsabilidad de los profesionales en calidad de prestatarios, se producen claras divergencias en torno al fundamento de esta responsabilidad.

Así, el Tribunal de Casación, en su sentencia de 12 de julio de 2012⁵⁸, sostiene que la responsabilidad de los facultativos o prestatarios, cuando acuden a materiales y dispositivos médicos necesarios para el ejercicio de su profesión, solo puede ser estimada cuando se aprecia negligencia en su actuación, dado que su función debe ser reconducida a sanar a sus pacientes de acuerdo

⁵⁶ “Salvo en el caso de que incurra en su responsabilidad por defecto de un producto sanitario, los profesionales de la salud mencionados en la parte cuarta de este código, así como cualquier establecimiento, servicio u organización en el que se realicen actos individuales de prevención, diagnóstico o atención sólo responden de las consecuencias perjudiciales de los actos de prevención, diagnóstico o atención en caso de culpa”.

⁵⁷ Así, CANTREAU, A.-S.: *Op. cit.*, p. 3.

⁵⁸ Cass. 1^a civ., 7-12-2012, n. 11-17510, Bol. Civ., n°165.

a las técnicas más apropiadas. Este parecer fue ratificado por un nuevo pronunciamiento del Tribunal de Casación (Cass. 1 civ.20-3-2013, n° 12, 12300).

En cambio, el 25-7-2013⁵⁹, el Consejo de Estado aprecia que la prestación médica realizada, con consecuencias perjudiciales para los usuarios de los productos y aparatos defectuosos, debe determinar la responsabilidad de sus facultativos, aun cuando no exista negligencia por su parte. Así, si se implanta en el curso de la prestación médica un producto defectuoso, como por ejemplo una prótesis de rodilla, el prestatario de ese servicio debe resultar responsable.

Con referencia ya a la consideración que en Alemania ha merecido la impresión 3D en medicina⁶⁰, constatamos en su doctrina especializada el progresivo auge que viene experimentando en la realidad sanitaria, en sus distintas aplicaciones, al considerarse que con el empleo de dicha tecnología se abren nuevas oportunidades para los pacientes. Se pone en evidencia así mismo, como fenómeno novedoso e intrínseco al uso del proceso de la bioimpresión, los distintos componentes o ámbitos (plan de diseño, empleo de materiales, soporte físico de impresión, etc.) que se necesita que converjan, a los efectos de posibilitar la impresión pretendida, y la consiguiente potencialidad de que dichos componentes puedan tener defectos que determinen daños a los pacientes.

Es precisamente en este último ámbito, el jurídico, donde la doctrina se muestra proclive a requerir convenientes reformas de adaptación del régimen legal que le sería aplicable, constituido, en lo fundamental, por la Ley de responsabilidad civil por productos defectuosos de 15 de diciembre de 1989 (ProdHaftG)⁶¹; normativa, cuya génesis fue la transposición de la Directiva

⁵⁹ CE, 25-7-2013, n. 339922, Falempin, *JCP* 2013, 1079 nota Paillard, 1359, n° 2.

⁶⁰ GRAF VESTPHALEN, F.: *Op. cit.* <https://www.fgvw.de/neues/archiv-2016/3d-druck-rechtliche-herausforderungen-durch-neue-technologien>; LEUPOLD, A./GLOSSNER, S.: *3D Printing. Recht, Wirtschaft und Technik des industriellen 3D-Drucks*, C.H. Beck, 2017, pp. 665 ss.; MIHALYI, J./MÜLLER, A-K.: “Legal aspects of bioprinted tissue and organs”, *INFORMATIK* 2016, Lecture Notes in Informatics (LNI), Gesellschaft für informatik, Bonn 2016, pp. 1637 ss.; LEUPOLD, A./GLOSSNER, S.: *3D-Druck, additive fertigung und rapid manufacturing*, Vahlen, 2016, pp. 9 ss.

En el seno de su doctrina, se apunta ya a la inminente implementación de la bioimpresión 4D, que permitirá la fabricación de estructuras con una precisión excepcional, superando las limitaciones de la bioimpresión 3D. Se afirma que la bioimpresión 4D conllevará un potencial generador de microestructuras que darán respuestas a numerosos estímulos, así como a diversos campos eléctricos y magnéticos. Se cree que, en un inminente plazo, revolucionará el campo de la ciencia biomédica y, en particular, los sectores específicos de la ingeniería de tejidos y de la medicina generativa. En este sentido VEERAVALLI, R.S./VEJANDLA, B./SAVANI, S./NELLURI, A./CHOWDARY PEDDI, N.: “Theree-Dimensional Bioprinting in Medicine: A comprehensive overview of current progress and challenges faced”, *Cureus*, 2023, jul. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10410602/>

⁶¹ Acerca de la misma, véase EHRING, P./TAEGER, J.: *Produkthaftungs- und Produktsicherheitsrecht*, Nomos, 1. Auflage 2022, pp. 119 ss; WAGNER, “Gesetz über die Haftung für fehlerhafte Produkte (1-

85/374. La razón, en lo esencial, debe hallarse en la interpretación restrictiva que acerca de la noción de producto -art. 2- se viene efectuando en el seno de la doctrina, y donde los de índole digital, no encuentran todavía, ni por vía análoga⁶², un adecuado encaje legal. No obstante, en ciertos supuestos de bioimpresión, algún componente podría revestir carácter independiente, respecto al resto que conforma el producto sanitario resultante, y con ello podría posibilitarse la responsabilidad civil del fabricante de aquel, de acuerdo a la noción de su art. 4. Se cita a este respecto, el caso del creador del archivo CAD que marca las directrices de control de la bioimpresión, si bien limitando la responsabilidad del creador o fabricante a los errores que provoque en el proceso final de impresión⁶³. Se considera que quien imprime el producto se convierte también en fabricante; es responsable de los errores en el producto final, independientemente de si se crearon en el archivo CAD, o no⁶⁴. Se propone no obstante, debido a la usual intervención de varios sujetos con distintas cometidos en el proceso de bioimpresión, que por vía contractual se pudieran fijar, con carácter previo, sus respectivas competencias, en aras a la posible determinación ulterior de sus respectivas responsabilidades⁶⁵.

A partir de la articulación del régimen de la ProdHaftG, convendría a nuestros efectos destacar la relevancia que revisten las previsiones que la misma dedica a la consideración del propio carácter defectuoso -art. 3-, o acerca del alcance de los daños -art. 1-, o del régimen de solidaridad entre los distintos fabricantes -art. 5-.

19 ProdHaftG), Münchener Kommentar BGB/ProdHaftG-beck-online, https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FMuekoBGB_Band5%2FProdHaftG%2Fcont%2FMuekoBGB.ProdHaftG.Band5.U16.T0.htm; MITTERHUBER, L.: "Grundzüge der Produkthaftung-Einblicke in theorie und praxis", *Zeitschrift für das Juristische studium*. www.zjs-online.com

Asimismo, tal como advierte SCHAEFER, D., deberá tenerse presente además la legislación sobre productos sanitarios, incorporada en la MPEUAnpG. (Ley de adaptación, en el ámbito nacional, de los productos sanitarios al Reglamento comunitario 2017/745) y donde a su amparo se podría generar responsabilidades en relación con los pacientes. "Roboterassistierte chirurgie und 3D-Drucker-risiken moderner technik richtig versichern", p. 4. <https://www.ecclesia.blog/roboterassistierte-chirurgie-und-3d-drucker-risiken-moderner-technik-richtig-versichern>

⁶² Así, con el producto intangible de la electricidad, que se recoge en su art. 2. Argumento, que según vimos, se utilizó en el marco del Derecho francés. En este sentido, BAUER, H.K./ Y OTROS.: *Op. cit.*, pp. 293 ss; HORST, A.: *Op. cit.*, pp. 61 ss.

El auge de la bioimpresión, está determinado también por la utilización generalizada de la impresión 3D en la sociedad, en sus distintas vertientes económicas. Véase a este respecto, las aportaciones monográficas siguientes: WIEBE, A.: *Op. cit.*, pp. 1 ss.

https://www.grur.org/uploads/tx_meeting/Wiebe_02.pdf ; MEYER, B./ Y OTROS.: *Op. cit.*, pp. 1 ss.

⁶³ KORTE/ISTREFF: "3D-Druck und Produkthaftung", *Der Betriebs*, pp. 2482 ss.

⁶⁴ SHAHINIAN, D.: https://www.mittelstandswiki.de/wissen/Haftung_beim_3D-Druck/, pp. 2-3.

⁶⁵ GRAF WESTPHALEN, F.: *Op. cit.*, pp. 4-6.; SCHAEFER, D.: *Op. cit.*, p. 2.

Debe tenerse en cuenta además que los productos sanitarios fabricados mediante impresión 3D requieren antes de su comercialización la supervisión, como organismo, de la Administración de Alimentos y Medicamentos (FDA). Su cometido es garantizar que los fabricantes cumplan con los requisitos legales de seguridad y eficacia. En definitiva, se trata de un control de índole administrativo en el producto sobre el que, en el caso de detectarse anomalías en el mismo, pueden generarse consiguientes responsabilidades, de igual forma como sucedía, según ya vimos, respecto al organismo supervisor, al amparo del Derecho español. En función del tipo de producto y de los riesgos que presenta, aparecen sistematizados en tres categorías. En particular, la FDA autoriza programas de software que están específicamente dirigidos a generar modelos 3D de la anatomía del paciente.

Si nos fijamos por último en el tratamiento que se ha efectuado en Italia, observamos como pauta común en las opiniones vertidas entre los especialistas del sector, la constatación de la progresiva utilización de la tecnología 3D en la fabricación de distintos productos⁶⁶, y en particular de la bioimpresión en relación con productos sanitarios⁶⁷.

Se considera que, ante los daños que se puedan generar al usuario como consecuencia del referido proceso de impresión, se debe acudir al marco legal que proporcionan los arts. 114-127 del Código del Consumidor; normativa que surgió como transposición de la Directiva 2008/374⁶⁸. Ciertamente, la doctrina que se ha dedicado a procurar la adaptación de la técnica de la bioimpresión, con sus singularidades (diversidad de compontes y potenciales responsables) a las previsiones contenidas en el referido Código, resaltando las indudables dificultades de integración de la la referida técnica en el concepto de producto y fabricante (art.115).

Aun invocando una interpretación flexible e integradora, se considera imprescindible una urgente reforma relacionada con los productos digitales, así como la incorporación de criterios acerca de la autonomía o accesoriedad

⁶⁶ Véase a este respecto CAERAN, M.:

https://www.academia.edu/23479298/LA_DIGITALIZZAZIONE_DEL_PRODOTTO_DIFETTOSO_STAMPA_3D_E_RESPONSABILIT%C3%80_CIVILE_MIRCO_CAERAN; PARZIALE, A./ COMANDÉ, G.: “Stampa 3D e fab tra quarta rivoluzione industriale e rischi di danno: il ruolo della responsabilità civile”, *Opinio Juris in Comparatione. Studies in comparative and national law*, Vol.1, n. 1/2018, pp. 1 ss.; MELILLO, M.: “La leggi e le linee guida per l’uso della stampa 3D nella sanità italiana”, pp. 2 y ss.

<https://www.techeconomy2030.it/2021/09/03/le-leggi-e-le-linee-guida-per-luso-della-stampa-3d-nella-sanita-italiana/>

⁶⁷ RIZZO, M. L.: “Bioprinting, dove sono le responsabilità”, 2016, <https://www.01health.it/tecnologie/stampa-3d/bioprinting-dove-sono-le-responsabilita>; VILLA, E.: *Op. cit.*, pp. 3 y ss.

⁶⁸ Véase a este respecto MONTINARO, R.: “Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law”, *Persona e Mercato* 2020/4, pp. 1 ss.

de estos⁶⁹. Ello conlleva una indudable repercusión en la responsabilidad civil que pudiera suscitarse a través de la bioimpresión, en su ulterior traslado acerca del carácter autónomo, o no, de ciertos productos sanitarios. Se pone de relieve, además, la necesidad de dar cumplimiento, con carácter previo, a los certificados de conformidad, de acuerdo al Reglamento 2017/745 de los productos sanitarios.

2.3.2. Problemática en el Derecho español. Repercusiones de las normativas europeas acerca de la bioimpresión como producto defectuoso y del uso de las nuevas tecnologías: Su explícita consideración

Debe tenerse presente, en primer lugar, que la regulación sobre responsabilidad civil por bienes o servicios defectuosos, contenida en los arts. 128-149 del Texto Refundido de la Ley General de Defensa de Consumidores y Usuarios de 16-11-2007, supuso la trasposición en nuestro país de la Directiva 1985/374. Al amparo de aquella regulación, y más concretamente de la noción de producto contenida en el art. 136⁷⁰, se han venido suscitando en la doctrina, con carácter general, discusiones en torno a si debía estarse a una concepción amplia de la citada noción, integradora de productos digitales, o si en cambio habría que defender una interpretación más restringida sustentada en la propia literalidad del precepto. De forma creciente, se ha venido imponiendo la primera de las referidas posiciones amparada en muy diversos argumentos⁷¹.

Por lo que respecta al proceso de la bioimpresión, en su consideración, en lo fundamental, de producto sanitario, la cuestión tal y como expusimos, ya quedó resuelta a favor de su cobertura legal, dado que desde la aprobación del Reglamento 2017/745 de productos sanitarios e inclusión de concretas variantes digitales, su normativa debía tenerse en cuenta, por su especificidad, con respecto a la que fue incorporada con carácter general por la Directiva 1985/374, y donde los productos sanitarios no son más que una concreta variante de productos.

Pues bien, esta argumentación encuentra idéntica justificación en su traslación a nuestro país. Por una parte, porque con ocasión de la regulación

⁶⁹ *Ibid.*, pp. 2-3.

⁷⁰ “A los efectos de este capítulo se considera producto cualquier bien mueble, aún cuando esté unido o incorporado a otro bien mueble o inmueble, así como el gas y la electricidad”.

⁷¹ En este sentido MARIN SALMERON, A.: “Algunas reflexiones sobre la propuesta de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos”, en *Contratación en el entorno digital* (Coord. Isabel González Pacanowska/M^a Carmen Planes Arnaldos), 2023, p. 399. Véase a este respecto la completa exposición del estado de la cuestión que efectúa el autor en pp. 396-407.

específica incorporada por RD 192/2023, de 21 de marzo, sobre productos sanitarios, y sin desconocer la aplicación directa del Reglamento 2017/745, se consideró incluso necesaria una explícita remisión de aquella acerca del alcance de la noción de producto sanitario a lo previsto a este respecto en la normativa comunitaria, y donde, como se sabe, sus potenciales componentes digitales (característicos del proceso de la bioimpresión) estuvieron muy presentes en la redacción por el legislador. Y por otra, se siguió, en lo concerniente a la responsabilidad civil por productos defectuosos, reproduciendo en el art. 136 del TRLGDCU la noción que de producto se contempló en la Directiva 1985/374.

Aun con todo, no debe desconocerse que en fechas recientes han sido aprobadas ciertas normas comunitarias, donde en el concepto de producto, tal y como se reivindicaba por la doctrina, ya se recogen las variantes digitales. A nuestros efectos, tales incidencias comunitarias no vienen sino a corroborar legalmente, en lo esencial, los componentes digitales que en relación con el proceso de la bioimpresión ya encontraban su plasmación en normas sobre productos sanitarios, y todo ello a los efectos de poder generar, si se cumplieran las exigencias vistas, nuevas responsabilidades de los fabricantes concurrentes en el proceso de la bioimpresión por los defectos que pudieran tener sus respectivos componentes.

En lo esencial, dicha incidencia europea está protagonizada por la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos⁷², donde por primera vez, aunque sea en sede de sus considerandos, se hace referencia al proceso de la bioimpresión. Asimismo, aun de forma incidental, por su validez en ciertos aspectos puntuales, debe traerse a colación también el Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024 (DOUE, n° 1689, de 12 de julio de 2024) por el que se establecen normas armonizadas en materia de inteligencia artificial. No obstante, la Propuesta de Directiva sobre producto defectuosos, en función del propio carácter de la norma, requerirá -tras su definitiva aprobación- una ulterior transposición por los respectivos países, debiéndose llevar a cabo, según su art. 22, en el plazo de un año, tras su entrada en vigor. Ello hace que la regulación que proporciona el TRLGDCS en sus art. 128-149 deba estar todavía muy presente en dicho intervalo temporal, como de igual forma ocurrirá en los distintos países hasta que no se produzca la referida trasposición de la nueva Propuesta de Directiva.

⁷² Mediante Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, el texto legislativo tramitado propuesto fue aprobado -en primera lectura- por el Parlamento, trasladándose al Consejo para su consideración. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_ES.pdf

Pues bien, a partir de tales incidencias legales, convendría detenernos en considerar dentro de las distintas previsiones legales que se incorporan, las que podrían incidir exclusivamente en el proceso de la bioimpresión, como determinante de la causación de daños en el usuario o paciente.

Así, en primer lugar, el art. 4.1 de la nueva Propuesta de Directiva identifica ya como producto a “cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos”, puntualizando que también lo sería “la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos”. En puridad, dicha previsión legal reproduce parcialmente la noción que de producto defectuoso viene conteniendo la vigente Directiva, con la adición, en particular, de las materias primas, archivos de fabricación digital y programas informáticos. El alcance resultante de estos dos últimos productos ya se obtenía, en lo esencial, de la consideración del proceso de bioimpresión como producto sanitario, en función de las normas que de esta última noción, según hemos ido analizando, se contemplan en su Derecho regulador. Por ello, a nuestros efectos, no reviste una novedad del mismo relieve que en otros sectores donde, a consecuencia de la defectuosidad del producto, se causan daños. Sí que deben reconocerse, no obstante, los importantes condicionantes que se acompañan a los citados archivos digitales⁷³ respecto a los programas informáticos,⁷⁴ en aras

⁷³ A este respecto, debe tenerse presente que dichos archivos digitales, para que tengan la consideración de producto sanitario a nuestros efectos, deben perseguir como objetivo, según vimos, una finalidad pretendida en el ámbito del art. 2 del Reglamento de producto sanitario 2017/745 (sea de diagnóstico, seguimiento, tratamiento, etc.) y por ello no basta con que tenga una finalidad de almacenar o transmitir datos de índole médico.

Dentro de este contexto, se encontrarían las afirmaciones contenidas en el considerando 16 de la Propuesta de Directiva, donde, aún situándose en un marco general, se hace mención (por primera vez) al proceso de impresión 3D: “Dado que los archivos digitales como tales no son productos incluidos en el ámbito de aplicación de la presente Directiva, los archivos de fabricación digital, que contienen la información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas, como taladros, tornos, molinos e impresoras 3D, deben considerarse productos, a fin de garantizar la protección de las personas físicas en los casos en que esos archivos sean defectuosos. Por ejemplo, un archivo defectuoso de diseño asistido por ordenador utilizado para crear un bien impreso en 3D que cause daños debe dar lugar a responsabilidad en virtud de la presente Directiva cuando dicho archivo se desarrolle o suministre en el transcurso de una actividad comercial...”.

El art. 4.2 de la Propuesta de Directiva se limita a calificar al archivo de fabricación digital como “una versión digital o plantilla digital de un bien mueble, que contine la información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas”.

⁷⁴ Los programas informáticos no incorporan, en cambio, ninguna definición. Tan solo el considerando 13 se limita a especificar algunas de sus aplicaciones: los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de inteligencia artificial. En su consideración de producto, resulta irrelevante, en principio, si se suministra a través de un modelo de programa informático físico, como servicio, o a través de la tecnología de la nube. Sin embargo, debe tenerse

a su categorización como producto digital, y con ello determinación de responsabilidades civiles por su carácter defectuoso. Todo ello revestirá especial utilidad en su traslado al proceso de bioimpresión, al ser usual la utilización de dichos componentes digitales hasta llegar a la impresión definitiva⁷⁵.

En segundo lugar, importaría precisar en relación con la hipótesis ya mencionada de que el producto sanitario resultante de la bioimpresión tras ser “introducido en el mercado” o “puesto en servicio”, y obtenida su correspondiente “evaluación de conformidad” (art. 2 del Reglamento 2017/745, apartados 27, 28 y 40)⁷⁶, hubiere sido susceptible de modificaciones ulteriores. Pues bien, la Propuesta de Directiva, en consonancia con lo que ya se afirmó al amparo de la regulación de productos sanitarios, mantiene el criterio coincidente de otorgarle carácter autónomo e independiente al producto, si la modificación operada en el mismo se considera sustancial⁷⁷, se lleva a cabo

presente la restricción contenida en su art. 2.2 (y considerando 14) al establecer que la directiva no se aplique a los programas informáticos libres y de código abierto desarrollados o suministrados al margen de una actividad comercial. En cambio, como se advierte asimismo en su considerando 14, cuando los programas informáticos se suministran a cambio de un precio, y por tanto consecuencia del desarrollo de una actividad comercial, se considera que procedería la aplicación de la Directiva.

Véase a este respecto ATIENZA NAVARRO, M.L.: “¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)”, *InDret*. 2.2023, pp. 9-10; MARTÍN CASALS, M.: “La propuesta de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”, *InDret*. 3.2023, pp. 18-9; IZQUIERDO GRAU, G.: “Software y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de software o de sistemas de inteligencia artificial”, *Revista de Internet, Derecho y política*, n° 38 (octubre, 2023), pp. 4-5.

<https://dialnet.unirioja.es/servlet/articulo?codigo=9087345>; GÓMEZ LIGUERRE, C.: “La propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos”, Editorial, *InDret*. 4. 2022, I-VII.

⁷⁵ Debe tenerse en cuenta lo que determina, si bien con carácter general, el art. 8.1 b) de la Propuesta de Directiva acerca de que los Estados miembros garantizarán que cuando un componente defectuoso haya provocado que el producto sea defectuoso, el fabricante del componente defectuoso también pueda ser considerado responsable de los mismos daños. En particular, se determina la responsabilidad del fabricante de un componente defectuoso, cuando dicho componente “esté integrado en un producto bajo su control, o esté interconectado con él”, y haya causado que dicho producto sea defectuoso.

⁷⁶ Tales delimitaciones (“introducción en el mercado”, “puesta en servicio”, “evaluación de conformidad”), son integradas en el Reglamento (UE) de 2024/1689, de Inteligencia Artificial, con ocasión de la implantación de un sistema de IA (art.3, apartados 9, 11, 20).

⁷⁷ De acuerdo al art. 4(18) de la Propuesta de Directiva, reviste la consideración de sustancial: “Toda modificación de un producto después de su introducción en el mercado o su puesta en servicio: a) Que se considera sustancial con arreglo a las normas nacionales o de la Unión aplicables en materia de seguridad de los productos, o b) cuando las normas nacionales de la Unión en materia de los productos no establezca ningún umbral sobre lo que debe considerarse una modificación que: i) cambie el rendimiento, la finalidad o el tipo originales del producto, sin que dicho cambio se haya previsto en la evaluación inicial de riesgos del fabricante, y ii) cambie la naturaleza del peligro, genere un nuevo peligro o aumente el nivel de riesgo”.

fuera de control del fabricante originario, y posteriormente lo comercializa o lo pone en servicio (art. 8.2) ⁷⁸.

En tercer lugar, debe tenerse presente, ante un proceso 3D de bioimpresión que ocasiona daños, las especiales dificultades, dada su complejidad técnica, para demostrar por parte del perjudicado, con carácter general, el carácter defectuoso del producto, como asimismo el nexo causal con sus daños sufridos.

Ciertamente, las previsiones legislativas contenidas en los art. 9 (exhibición de pruebas) y art. 10 (carga de la prueba), de la Propuesta de Directiva pueden facilitar la reparación indemnizatoria que se pretende. En síntesis, a través del art. 9 se reconoce la posibilidad, a petición de la persona perjudicada que presenta hechos y pruebas que respaldan la verosimilitud de su reclamación, de que el órgano judicial deba acordar que el demandado fuera el que debiera aportar las pruebas pertinentes de que disponga, si bien debiéndose reconducir a las que pudieran ser necesarias. Además, con la particularidad, según dispone su art. 10 (apartado 2a) de que, si el demandado incumpliera tal cometido, se partiría en tal caso de la presunción del carácter defectuoso del producto.

Sin perjuicio de que el órgano judicial pueda acordar la exhibición de pruebas por parte del demandado, de acuerdo al art. 9, con las consecuencias referidas, se puede acudir directamente por el órgano judicial a la presunción del carácter defectuoso del producto, en función de lo dispuesto en art. 10.4,

Dentro de este contexto, a nuestros efectos, se encontraría el segundo inciso del considerando 40: "...Cuando una modificación sustancial se realice a través de una actualización o mejora de un programa informático, o por el aprendizaje continuo de un sistema de IA, debe considerarse que el producto sustancialmente modificado se comercializa o pone en servicio en el momento en que se introduzca realmente la modificación".

Con referencia a la implantación de un sistema de IA, el Reglamento Europeo de Inteligencia Artificial incorpora en su art. 3, apartado 23, una completa delimitación de modificación sustancial: "un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectada el cumplimiento por parte de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate".

⁷⁸ En este sentido NAVAS NAVARRO, S.: "Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial", *Revista Cesco de Derecho de Consumo*, n° 44/2022, pp. 42-45; ATIENZA RODRÍGUEZ, M.L.: *Op. cit.*, pp. 25-6. Asimismo partiendo de la premisa de cambios sustanciales, LÓPEZ TUR, T. advierte de su incidencia en los casos de inteligencia artificial: "Especialmente interesante resulta la introducción de la posibilidad de exigir responsabilidad a aquel que modifique el producto, puesto que en casos de inteligencia artificial con sistemas de autoaprendizaje o posibilidad de que el operador que hace uso de la IA modifique el producto que finalmente recibe el consumidor puede ser considerado fabricante a todos los efectos de la responsabilidad por daños causados por productos defectuosos". "Producto defectuoso e impresión de prótesis con impresión 3D", en *Derecho y Medicina: Desafíos tecnológicos y científicos* (Direct. Cristina Gil Membrado), Dykinson, 2023, p. 60.

cuando dicho órgano considere que el demandante se enfrenta a dificultades excesivas en la probanza de la defectuosidad del producto -por su complejidad técnica o científica- como asimismo de su nexo causal con los daños que se le han producido, si bien sobre la base de que el demandante acredite con pruebas pertinentes ciertos extremos de verosimilitud⁷⁹. Ciertamente, esta posibilidad, sustentada en lo esencial en la discrecionalidad judicial, podrá tener especial utilidad en el procedimiento de bioimpresión, por la complejidad técnica que lleva implícita.

En cuarto y último lugar, en lo respecta a otros aspectos a destacar del régimen jurídico que se incorporan con la Propuesta de Directiva y que podrían tener virtualidad en relación con el producto resultante de la bioimpresión, resaltaríamos dos. Por una parte, partiendo del carácter autónomo e independiente de los componentes o productos sanitarios intervinientes en el proceso de bioimpresión: el régimen de solidaridad que se incorpora, respecto a los respectivos fabricantes, en el art. 12.1 de la Propuesta de Directiva⁸⁰. Se trata de un régimen aplicable desde hace ya algunos años, bajo la cobertura de la Directiva de 25 de julio de 1985, y justificable no solo por ser de mayor protección para la víctima, sino también por encontrarse cada componente o producto sanitario que converge en el proceso bajo el único control de su respectivo fabricante.

Por otra parte, partiendo de la regulación que acerca de las causas de exoneración recoge el art. 11 de la Propuesta de Directiva, extensible a los fabricantes de la bioimpresión, merecen destacarse las consideraciones que efectúa sobre la irrelevancia de la posible invocación de las mismas cuando el carácter defectuoso del producto se suscita en ciertos extremos del mismo donde se considera que todavía no reviste carácter autónomo respecto al fabricante inicial, al permanecer todavía bajo su control. Ello se particulariza, en relación con la existencia de “un servicio conexo; programas informáticos, incluidas las actualizaciones o mejoras de programas informáticos; o la falta de actualizaciones o mejoras de los programas informáticos necesarias para mantener la seguridad, o una modificación sustancial del producto”.

⁷⁹ “Que el demandante demuestre que es probable que el producto sea defectuoso o exista un nexo causal entre el carácter defectuoso del producto y el daño o ambos”. No obstante, se le reconoce al demandado el derecho a impugnar la existencia de las referidas dificultades excesivas invocada por el demandante.

⁸⁰ “Sin perjuicio de las disposiciones nacionales en relación con los derechos de división de la responsabilidad o de repetición, los Estados miembros garantizarán que, cuando dos o más operadores económicos sean responsables de los mismos daños con arreglo a la presente Directiva, puedan ser considerados responsables solidarios”. En conexión con este último régimen se contempla el derecho de repetición en el art 14.

Véase, a este respecto ATIENZA RODRÍGUEZ, M.L.: *Op .cit.*, p. 27; MARTÍN CASALS, M.: *Op. cit.*, pp. 27-29.

BIBLIOGRAFÍA

- ÁLVAREZ OLALLA, P.: “Daños causados al paciente por utilización de un producto sanitario defectuoso. Al hilo del caso Ala Octa”, *RCDI*, 2022, n° 794, pp. 3366 ss.
- ARANDA BAULERO, M.: “Un cambio en los paradigmas de los sistemas de salud, la tecnología 3D”; *Revista Peruana de Investigación en Salud*, vol. 4, n.3, 2020, pp. 121. <https://www.redalyc.org/journal/6357/635767700005/html/>
- ATIENZA NAVARRO, M.L.: “¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)”, *InDret*. 2. 2023, pp. 1 ss.
- BAENA, J.M.: “Medicina regenerativa y bioimpresión 3D de tejidos y órganos”, <https://trepanos.es/2024/01/22/medicina-regenerativa-y-bioimpresion-3d-de-tejidos-y-organos/>
- BAUER, H.K./HELLER, M./FINK, M./MARESCH, D./GARTNER, J.: “Social and legal frame conditions for 3D (and) bioprinting in medicine”, *International Journal of Computerized Dentistry*, 2016, 19 (4), pp. 293 ss.
- BISHOP, E S./MOSTAFA, S/PAKVASA, M./ LUU, H.H./LEE, M.J./WOLF, J.M./AMEER, G.A./HE, T.C./REID, R.R.: “3-D bioprinting technologies in tissue engineering and regenerative medicine: current and future trends” <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6003668>
- BOLGIANI, A./ HERMIDA, E.: “Bioimpresión 3D en piel”, *Cirugía plástica ibero-latinoamericana*, vol. 46, abril 2020. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0376-78922020000200014&lng=es&nrm=iso&tlng=es
- CAERAN, M.: *La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile*, University of Trento, The trento Law and Technology Research Group Student Paper, n. 24, 2016, https://www.academia.edu/23479298/LA_DIGITALIZZAZIONE_DEL_PRODOTTO_DIFETTOSO_STAMPA_3D_E_RESPONSABILIT%C3%80_CIVILE_MIRCO_CAERAN
- CANTREAU, A.-S.: “Bioimpression: quelles responsabilités en cas de dommage”, <https://www.alain-bensoussan.com>
- CÉSAR-JUÁREZ, A.A./ OLIVOS-MEZÁ, A./LANDA -SOLÍS, C./CARDENAS SORIÁ, V.H./SURIEL SILVA-BERMUDEZ, P./SUÁREZ ABEDO, C./OLIVOS DÍAZ, B./IBARRA-PONCE DE LEON, J.C.: “Uso y aplicación de la tecnología de impresión y bioimpresión 3D en medicina”, *Revista de la Facultad de Medicina de la UNAM*, Vol. 61, n. 6, noviembre-diciembre 2018. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0026-17422018000600043
- CIRULLI, A./BORGHETTI-CARDOSO, L./TORRAS, N./MARTÍNEZ, E.: “Mimicking human skin constructs using nonporous-pullulan-based hydrogels”, *International Journal of Bioprinting* 3395, DOI: <https://doi.org/10.36922/ijb.3395>
- COUCKE, P.: “La médecine du futur. L’impression 3D en santé (1ère partie): Les structures à fonction non vitale”, 2019. <https://orbi.uliege.be/bits->

tream/2268/268678/1/La%20m%C3%A9decine%20du%20futur%201%27impression%203D%20en%20sant%C3%A9%20les%20structures%20%C3%A0%20fonction%20non%20vitale.pdf

- DEKEUWER-DEFOSSEZ, F.: “Réflexions sur l’acte médical non thérapeutique”, in *Mélanges en l’honneur de Gérard Mémèteau, Droit médical et éthique médicale: regards contemporains*. Sous la dir. de J. Leonhard, B.P et F.Vialla, vol 1, 2015, pp. 399 ss.
- EHRING, P./TAEGER, J.: *Produkthaftungs-und Produktsicherheitsrecht*, Nomos, 1.Auflage 2022, pp. 119 ss.
- GALÁN CORTÉS, J.L.: *Responsabilidad civil médica*, Civitas, Cizur Menor (Navarra), 2022.
- GARANT-AUBRY, J./LÉGER-RIOPEL, N.: “L’imprimante 3D et le domaine de la santé: enjeux juridiques et éthiques”, 2016. <https://www.chairesante.ca/articles/2016/limprimante-3d-et-le-domaine-de-la-sante-enjeux-juridiques-et-ethiques/>
- GARCÍA GIL, M.: “Los retos que plantea la biotecnología al Derecho Privado. La Bioimpresión y el Bioderecho”, 2016. <https://repository.upb.edu.co/handle/20.500.11912/2774>
- GARCÍA MICÓ, T.G.: *La robótica quirúrgica y Derecho de Daños*, Marcial Pons, Madrid, 2024.
- GRAF WESTPHALEN, F.: “3D-Druck: Rechtliche Herausforderungen durch neu Technologien”, 2016. <https://www.fgw.de/neues/archiv-2016/3d-druck-rechtliche-herausforderungen-durch-neue-technologien>
- GRIMALT SERVERA, P.: “La responsabilidad (civil o patrimonial) del personal médico de los centros sanitarios y de las administraciones sanitarias por los daños causados por un producto sanitario defectuoso”; *Bioderecho*. es, núm. 17, enero-julio 2023. <file:///C:/Users/Usuario/Downloads/Responsabilidad+por+productos+sanitarios+defectuosos.pdf>
- GÓMEZ LIGUERRE, C.: “La propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos”, Editorial, *InDret* 4. 2022, I-VII.
- HORST, A.: “Bald Organe aus dem Drucker?”, Zehn, april 2017, *Rescriptum, Münchner studentische Rechtszeitschrift*, pp. 61 ss.
- IZQUIERDO GRAU, G.: “Software y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de software o de sistemas de inteligencia artificial”, *Revista de internet, derecho y política*, n° 38 (octubre, 2023), pp. 1 ss. <https://dialnet.unirioja.es/servlet/articulo?codigo=9087345>
- JAIN, P./KATHURIA, H./DUBEY, N.: “Advances in 3D bioprinting of tissues/organs for regenerative medicine and-in-vitro models”, 2022. <https://www.sciencedirect.com/science/article/abs/pii/S0142961222002794>
- JORCANO NOVAL, J.L.: “Informes anticipando bioimpresión en la medicina del futuro”. *Observatorio de tendencias de medicina personalizada de precisión. Fundación Instituto Roche* (Coord. Por J.L. Jorcano Noval), 2019. https://www.institutoroche.es/static/archivos/Informes_anticipando_BIOIMPRESION_digital.pdf

- KIRILLOVA, A./BUSHEV, A./ABUBAKIROV, A./SUKIKH, G.: “Bioethical and Legal Issues in 3D bioprinting”, *International Journal of Bioprinting* (2020), v. 6, I, 3, https://www.academia.edu/55980098/Bioethical_and_Legal_Issues_in_3D_Bioprinting
- KORTE/ISTREFI: “3D-Druck und Produkthaftung”, *Der Betriebs*, pp. 2482 ss.
- LEE, I.Y./SALAS-SÁNCHEZ, F./POMARES-WAUTERS, G./RAMOS-GAMBOA, M.F./GODFREY-LOWIS, M./MORA-ROMÁN, J.J.: “Bioimpresión de órganos y tejidos en tercera dimensión: técnicas, aplicaciones y limitaciones”, https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S0379-39822018000300041&lng=en&nrm=iso&tlng=es
- LE GOFFIC, C.: “Impression 3D et responsabilité”, *Journal du Droit de la Santé et de l'Assurance-Maladie* (JDSAM), 2016/2, n°14, pp. 17 ss. <https://shs.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance-maladie-2016-2-page-17?lang=fr>
- LEQUILLERIER, C.: “Impression 3D et santé: Le possible interventionnisme du droit face au transhumanisme”, *Journal de Droit de la santé et de l'Assurance-Maladie*, 2016, n. 14, pp. 12-16. <https://shs.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance-maladie-2016-2-page-12?lang=fr>
- LEUPOLD, A./GLOSSNER, S.: *3D Printing Recht, Wirtschaft und Technik des industriellen 3D-Drucks*, C.H. Beck, 2017, pp. 665 ss.
- *3D-Druck, additive fertigung und rapid manufacturing*, Vahlen, 2016.
- LOO GIL., C.: “Bio impresión 3D: importancia en la actualidad”, *TecnoHumanismo, Revista Científica*, febrero, 2021, volumen 1/No.1, pp. 87 ss. <https://tecnohumanismo.online/index.php/tecnohumanismo/article/view/2>
- LÓPEZ TUR, T.: “Producto defectuoso e impresión de prótesis con impresoras 3D”. En *Derecho y Medicina: desafíos tecnológicos y científicos* (Direct. Cristina Gil Membrado), Dikynson, 2023, pp. 45 ss.
- MARÍN SALMERÓN, A.: “Algunas reflexiones sobre la propuesta de modificación de la directiva sobre responsabilidad por los daños causados por productos defectuosos”, en *Contratación en el entorno digital* (Coord. Isabel González Pacanowska/Maria Carmen Planas Arnaldos) 2023, pp. 391 ss.
- MARTÍN CASALS, M.: “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”, *InDret*.3.2023, pp. 55 ss.
- MELILLO, M.: “La legge e le linee guida per l'uso della stampa 3D nella sanità italiana”, <https://www.techeconomy2030.it/2021/09/03/le-leggi-e-le-linee-guida-per-luso-della-stampa-3d-nella-sanita-italiana/>
- MENCACCI, M.: “Stampa 3D nel futuro della sanità: eco gli usi pratici e i vantaggi”, <https://www.agendadigitale.eu/sanita/stampa-3d-nel-futuro-della-sanita-ecco-gli-usi-pratici-e-i-vantaggi/>
- MEYER, B./SCHREIBER, S./SCHMAUDER, M./HÖHN, K./HILGERS, L.: “3-D-Druck und Produktsicherheit:Informationen für Hersteller und andere

- geschäftsmäßige Nutzer”, Baua:Focus, november 20.8, pp. 1 ss. DOI: 10.21934/baua:fokus20181121 <https://www.baua.de/DE/Angebote/Publikationen/Fokus/3-D-Druck-Produktsicherheit>
- MIHALYI, J./MÜLLER, A-K.: “Legal aspects of bioprinted tissue and organs”, INFORMATIK 2016, Lecture Notes in Informatics (LNI), Gesellschaft für informatik, Bonn 2016, pp. 1637 ss.
- MITTERHUBER, L.: “Grundzüge der Produkthaftung-Einblicke in theorie und praxis”, *Zeitschrift für das Juristische studium*, www.zjs-online.com
- MONTINARO, R.: “Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law”, *Persona e Mercato* 2020/4, pp. 1 ss.
- MONTMARTÍN, M./MEYER, C./ PAZART, L.: “L’impression 3D à l’hôpital: quelle réglementation en France”, *Revue de Stomatologie, de Chirurgie Maxilo-Faciale et de Chirurgie Orale*, V. 116, n. 5, 2015, pp. 302 ss. <https://www.sciencedirect.com/science/article/pii/S2213653315000737>
- NAVAS NAVARO, S.: “Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial”, *Revista Cesco de Derecho de Consumo*, n° 44/2022, pp. 27 ss.
- ORTIZ GIL, A.: “Las impresoras 3D como herramientas científicas”. En *Encuentros Multidisciplinares. Observatori Astronomic de la Universitat de Valencia*, n° 61, 2019, p. 1 ss. https://repositorio.uam.es/bitstream/handle/10486/687514/EM_61_6.pdf?sequence=1&isAllowed=y
- PARICARD, S.: “Consentement aux actes médicaux non thérapeutiques”, in *Consentement et santé*. Sous la dir. de l’Association française de droit de la santé, Dalloz, 2014, pp. 103 et ss.
- PARZIALE, A./COMANDÉ, G.: “Stampa 3D e fab la tra quarta rivoluzione industriale e rischi di danno: il ruolo della responsabilità civile”, *Opinio Juris in Comparatione. Studies in comparative and national law*, Vol 1, n. 1/2018, pp. 1 ss.
- RICCOMANO, A.: “La stampa 3D al servizio della salute”, <https://trendsanita.it/stampa-3d-salute/>
- RIZZO, M.L.: “Bioprinting, dove sono le responsabilità”, 2016. <https://www.01health.it/tecnologie/stampa-3d/bioprinting-dove-sono-le-responsabilita/>
- ROBERT GUILLÉN, S.: “Marco regulador de la impresión y bio-impresión 3D para la aplicabilidad médica. Cuestiones sobre la patentabilidad de los productos de la bio-impresión 3D”. En *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 Covid 19*. Susana Navas Navarro (dir.) Ed. Comares, 2021.
- SCHAEFER, D.: “Roboterassistierte chirurgie und 3D-Drucker-risiken moderner technik richtig versichern”, 2020. <https://www.ecclesia.blog/roboterassistierte-chirurgie-und-3d-drucker-risiken-moderner-technik-richtig-versichern>
- SHAHINIAN, D.: “Wer für 3D-gedruckte Bauteile haftet” https://www.mittelstandswiki.de/wissen/Haftung_beim_3D-Druck/

- THIEULIN, C.: “Grâce à la bio-impression 3D, la greffe de peau est en pleine révolution”, 2024. <https://www.slate.fr/story/266037/bio-impression-3d-greffe-peau-traitement-brulures-medecine-recherche-technologie-revolution>
- TOMORROW BIO: “Bioimpresión 3D: Un puente en los trasplantes de órganos”, 18-7-2023. <https://www.tomorrow.bio/es/post/la-bioimpresion-3d-como-puente-para-los-trasplantes-de-organos-2023-06-4727432548-3d-printing>
- “L’impatto delle protesi stampate in 3D sulla sanità moderna”, <https://www.tomorrow.bio/it/post/l'impatto-delle-protesi-stampate-in-3d-sulla-sanita-moderna-2023-06-4727444136-3d-printing>
- VEERAVALLI, R.S./ VEJANDLA, B./ SAVANI, S./NELLURI, A./CHOWDARY PEDDI, N.: “Theree-Dimensional Bioprinting in Medicine: A comprehensive overview of current progress and challenges faced”, *Cureus*, 2023, jul. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10410602/>
- VERMEULEN, N./HADDON, G./SEYMOUR, T./FAULKNER-JONES, A./SHU, W.: “3D Bioprint me: a socioethical wiew of bioprinting human organs and tissue”, 2017. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5827711/>
- VILLA, E.: “Stampa 3D in sanità: esempi e soluzioni per ospedali e strutture sanitarie”, 2023. <https://www.healthtech360.it/salute-digitale/stampa-3d-sanita-esempi-soluzioni/>
- WAGNER: “Gesetz über die Haftung für fehlerhafte Produkte (1-19 ProdHaftG), *Münchener Kommentar BGB/ProdHaftG-beck-online*, 2004. https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FMuekoBGB_Band5%2FProdHaftG%2Fcont%2FMuekoBGB.ProdHaftG.Band5.U16.T0.htm
- WIEBE, A.: *Inmaterialgüterrechtliche Aspekte des 3D-Drucks und Haftungsfragen*, Universität Göttingen, 2018. https://www.grur.org/uploads/tx_meeting/Wiebe_02.pdf
- WOLF, P.: “La bioimpression des avancées à petits pas”, <https://lecardiologue.com/la-bio-impression-des-avancees-a-petit-pas/>
- YAN, Y./XUEYAN, L./GAO, Y./BHATTACHARYYA, A./ZHAO, X./ZHANG, S.C.: “3D bioprinting of human neural tissues with functional connectivity”, *TECNOLOGIA*, V. 31, 2 [https://www.cell.com/cell-stem-cell/fulltext/S1934-5909\(23\)00439-3?_returnURL=https://linkinghub.elsevier.com/retrieve/pii/S1934590923004393](https://www.cell.com/cell-stem-cell/fulltext/S1934-5909(23)00439-3?_returnURL=https://linkinghub.elsevier.com/retrieve/pii/S1934590923004393)
- ZWETYENGA, N.: “L’impression 3D au service de la chirurgie”, *Journal de Droit de la santé et de l’assurance maladie*, 2016, n° 14, <https://www.institutdroitsante.fr>

Taxonomía de los modelos de IA de uso general. Probabilidad de generar riesgos de alto impacto y la necesidad de identificarlos

CARMEN MUÑOZ GARCÍA

Profesora Titular de Derecho Civil UCM

Codirectora de la Sección de IA del Spanish Hub (ELI)

Miembro del Instituto de Derecho Europeo e Interregional (IDEIR)

Sumario: 1. JUSTIFICACIÓN DEL ESTUDIO. 1.1. La IA Generativa como modelo de IA de uso general. El caso. 1.2. ¿Por qué regularlo? 1.3. La incidencia en los derechos de la persona. 2. TAXONOMÍA DE LOS MODELOS DE IA DE USO GENERAL. 2.1. Definiciones legales y clasificación. 2.2. La exigencia general de transparencia y una regulación singular para los modelos de GPAI. 2.3. Marco regulatorio propio. 2.3.1. Obligaciones y requisitos técnicos para los modelos de IA de uso general o «GPAI simple» . 2.2.2. Obligaciones y requisitos técnicos para los modelos de IA de uso general «con riesgo sistémico». 2.3.3. Los códigos de buenas práctica. 2.2.4. Otros artículos de aplicación. 3. EL RIESGO EN LOS MODELOS Y SISTEMAS GPAI 3.1. Definiciones sobre el riesgo. Identificar incidente y peligro de IA. 3.2. ¿A qué sujetos se dirigen las obligaciones de evitar el riesgo? ¿A qué herramientas? 4. REFLEXIONES FINALES. 5. BIBLIOGRAFÍA

1. JUSTIFICACIÓN DEL ESTUDIO

1.1. LA IA GENERATIVA COMO MODELO DE IA DE USO GENERAL. EL CASO

Los aspectos jurídicos a los que se refiere este capítulo¹ tienen ver con determinadas herramientas de inteligencia artificial generativa

¹ Este trabajo se enmarca en la Cátedra Internacional ENIA de «IA Generativa: retos y riesgos», financiada por la Unión Europea-Next Generation EU; en el Proyecto OdiseIA for GOOGLE.

(IAGen)² que, con el carácter de generalidad y flexibilidad para adaptarse a distintos fines y crear contenido multimodal, evolucionan a gran velocidad, son usados por millones de usuarios y se comportan de manera muy diferente. El máximo exponente lo encontramos con GPT -el modelo de IA de uso general-, y con ChatGPT -el sistema, en cualquiera de sus versiones-, con clara incidencia en los derechos de la persona.

Se trata de herramientas profusamente utilizadas a nivel mundial y que inciden, en su uso y desarrollo, en múltiples aspectos jurídicos que exceden las previsiones del Reglamento 2024/1689, de Inteligencia Artificial que, vigente en Europa desde el 1 de agosto de 2024³, se interrelaciona con normativas de privacidad, protección de datos, propiedad intelectual, derecho de consumidores o responsabilidad civil de los diferentes agentes que intervienen en su desarrollo y uso. Con todo, entiendo que esta materia se ha de considerar desde una perspectiva holística en su interacción con todos esos marcos regulatorios, y además, que habrán de complementarse con regulaciones específicas, resoluciones de los tribunales u otras actuaciones jurídicas.

No es asunto baladí, sino crucial en cuanto nos estamos refiriendo a grandes modelos de lenguaje generativos (LLMs, por sus siglas en inglés), denominados modelos de IA de uso general en la redacción definitiva del Reglamento de Inteligencia Artificial 2024/1689, de 13 de junio (RIA o LIA por sus siglas en inglés)⁴. Cabe citar entre otros, GPT⁵, LLaMA⁶

org «AI Governance» (subproyecto #1.1 «*Mapping of AI governance - recommendations and regulation*»); y en el Grupo de Investigación UCM 971680 «Derecho de Daños. Derecho de la contratación»

² La IA generativa es mucho más que un chatbot, es una denominación general para un ecosistema masivo de tecnologías vagamente relacionadas, que incluyen mucho más que chatbos de textos conversacionales, generadores de imágenes, asistentes de codificación o sistemas que componen música y crean videos. Así se expresan Katherine Lee, A. Feder Cooper, James Grimmelmann, «Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain», *Arxiv*, (15 septiembre 2023). Visto en <https://arxiv.org/abs/2309.08133>

³ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828. Es el Reglamento de Inteligencia Artificial (RIA o *AI Act*, por sus siglas en inglés), publicado en el DOUE de 12 de julio de 2024.

⁴ Su regulación específica se contempla en los artículos 51 a 56 del Reglamento (UE) 2024/1689. Si bien, habrá otros preceptos específicos a lo largo del texto.

⁵ Desde la irrupción en abierto del modelo, en noviembre de 2022, OpenAI ha lanzado varias versiones gratuitas -también de pago- del modelo GPT (versión 2, 3 ó 4o), según variaban capacidades, fuese más rápido e intuitivo y con mayor capacidad de razonamiento, incluso, si admite entradas y salidas de texto e imágenes, y es capaz de soportar video y audio en diferentes contextos.

⁶ LLaMA (*Large Language Model Meta AI*) es un gran modelo de lenguaje (LLM) lanzado por Meta AI en febrero de 2023. En julio de 2024, Meta ha lanzado Llama 3.1.405B, de código abierto, fácilmente descargable, también de conocimiento general, más operativo, con traducción multilingüe y en condi-

o Gemini -antes Bard-⁷, que sin ser *per se* sistemas de IA, precisan de su inserción en estos -incluso vía web-, como ChatGPT 4o, o Gemini Ultra -inicialmente, Google Bard-), por lo que también nos referimos a los sistemas de IA, principalmente a los de uso general, por constituir estos el binomio necesario para desplegar la enorme eficacia que son capaces de desarrollar.

Como a nadie escapa, no es ocioso poner de relieve que estos modelos de IA que han generalizado el uso de esta tecnología en muy poco tiempo a través de sistemas de IA (vía *ChatGPT*, *Copilot* o *Gemini*) -de acceso libre y gratuito en muchos casos, de uso global, con capacidad para crear contenidos y responder a múltiples fines-, mucho más allá de los incontables beneficios que proporcionan, son el origen de cientos de incidencias. En definitiva, que pueden vulnerar derechos fundamentales y poner en jaque el acervo o corpus jurídico de la Unión Europea.

Pero vayamos por partes, dentro de los modelos de IA de uso general, nos encontramos con la herramienta más generalizada y utilizada en esta primera fase de desarrollo global. Se trata de GPT (del acrónimo en inglés “Generative Pre-trained Transformer”)⁸. Esta herramienta que hace referencia: (i) al tipo de arquitectura de red neuronal artificial -“transformer”-; (ii) a los grandes modelos de lenguaje -LLM, por sus siglas en inglés-, diseñados para comprender y generar contenido como un ser humano -“generative”-; y (iii) que ha sido previamente entrenado con una técnica llamada aprendizaje automático, que es capaz de analizar infinitos datos para aprender patrones de lenguaje como si fuera un humano -modelo “pre-trained”-, es capaz de crear contenidos multimodales y multifuncionales, con incontables beneficios pero también con múltiples riesgos que esto conlleva.

Siendo GPT (el modelo) y ChatGPT (el sistema) la herramienta que democratizó el uso de la inteligencia artificial generativa⁹, y que alcanzó la cifra record de ser la aplicación de consumo que más rápidamente alcanza

ciones de competir con su principal adversario, GPT-4. Sobre el modelo Llama 3, la características desgarnadas por Meta en su presentación en abril de 2024 <https://about.fb.com/ltam/news/2024/04/presentamos-meta-llama-3-el-modelo-de-lenguaje-de-gran-tamano-mas-potente-hasta-la-fecha/>

⁷ Bard también es un gran modelo de lenguaje (LLM), creado por Google y diferente al modelo de GPT. Actualmente denominado Gemini (gemelos en latín), con su nueva denominación Google pretende mostrar la ambivalencia del modelo.

⁸ A diferencia del modelo de lenguaje generativo (LLM) utilizado por GPT, Bard de Google, utiliza el modelo de Lenguaje para Aplicaciones de Diálogo (LaMBDA). En definitiva, GPT y Bard son herramientas de procesamiento del lenguaje natural (NLP) que operan con distintas capacidades. Interesante la comparativa que ofrece el siguiente análisis <https://salesystems.es/google-bard-vs-chat-gpt/>

⁹ En el considerando 99 del Reglamento se especifica que: *los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general.*

máximos en número de usuarios¹⁰, nos serviremos de este instrumento cómo caso de uso para acercarnos a los modelos de IA de uso general, sin perder de vista su integración en los sistemas de IA de uso general.

Ahora bien, queda advertido que no hay impedimento para que los modelos de IA de uso general, y el sistema de IA de uso general, queden finalmente integrados en otros sistemas como los de alto riesgo, con las consecuencias y efectos que ello conlleva.

1.2. ¿POR QUÉ REGULARLO?

La profusión y el uso global de modelos de IA de uso general y de sistemas de IA de uso general, al alcance de cualquier ciudadano y con pretensiones no siempre adecuadas o lícitas, ha dejado al descubierto que del uso de este tipo de herramientas pueden derivarse graves consecuencias para los usuarios, e incluso, para terceros ajenos al uso directo de la herramienta (la manipulación cognitiva, la alteración del infraestructuras críticas -energía y agua-, el transporte, el sistema financiero o tributario, la manipulación del acceso al empleo o del acceso a prestaciones laborales, a servicios privados esenciales y a servicios y prestaciones públicos esenciales, son solo algunos de los cientos de ejemplos en los que se desarrolla la IA y en los que se opera con IA generativa). El trabajo del grupo de expertos de la OCDE. *AI*¹¹ *sobre incidentes de IA* (publicado en mayo de 2024), poco antes de la aprobación definitiva del RIA y de su publicación en el DOUE, da cumplida muestra de la variedad de riesgos reales y potenciales de esta tecnología disruptiva¹².

Con la regulación se pretende que estas herramientas de aprendizaje automático, entrenadas con grandes cantidades de datos, y destinadas a emular la inteligencia humana, se pongan en circulación, desarrollen y usen de manera uniforme en el mercado de la Unión, de conformidad con los valores, derechos fundamentales y principios de la UE, preservando y fomentando la

¹⁰ . En la actualidad, ChatGPT alcanza los 200 millones de usuarios activos semanales en todo el mundo. Ver la noticia en *El Derecho* (30 agosto 2024) <https://elderecho.com/chatgpt-de-openai-ya-tiene-200-millones-de-usuarios-activos-semanales>

¹¹ La OCDE presentó en mayo de 2024 *Monitor de incidentes de IA de la OCDE* sobre la importancia de la Metodología y divulgaciones de daños reales y probables del desarrollo y uso de la IA, no sin antes advertir que este paper se elabora tras monitorear noticias mundiales y que estos perjuicios, muy probablemente, sólo representen un subconjunto de todos los incidentes y peligros de IA en el mundo. <https://oecd.ai/en/incidents-methodology>

¹² Esto, habrá de considerarse con independencia de si el modelo opera en un sistema de IA de uso general o termina utilizándose en un sistema de alto riesgo.

innovación y el liderazgo en un complejo equilibrio de progreso tecnológico y salvaguarda de derechos¹³.

Y si el objetivo plasmado en el Reglamento europeo de Inteligencia Artificial 2024/1689, de 13 de junio (RIA) es que se facilite la inversión y la innovación en beneficio de las personas, también lo es que esta tecnología se desarrolle en el mercado único de manera ética, segura y confiable, centrada en el ser humano¹⁴. Se trata de garantizar la salud, la seguridad y los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección medioambiental.

Lo anterior no será fácil. Para ello, desde un primer momento se propone un enfoque regulatorio de los sistemas de inteligencia artificial basado en el riesgo, que proporciona normas vinculantes atendiendo al nivel de peligro o amenaza que pueda producir la herramienta a todos los derechos especialmente protegidos. En el artículo 3, apartado 2 del RIA se define el riesgo como: «la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio».

Lo que derivó, en la propuesta inicial, en una clasificación de sistemas de inteligencia artificial vinculados al nivel de riesgo que generan para las personas, los derechos fundamentales o los intereses públicos de la UE. Esta clasificación lleva a diferenciar los sistemas en: (i) «de riesgo inaceptable»; (ii) «de alto riesgo»; (iii) «de riesgo limitado o medio»; y (iv) «de riesgo bajo o mínimo». De esta regulación, rigurosa y proporcional al riesgo que la herramienta representa, quedaban al margen de normativización específica los modelos de IA de uso general.

¹³ Así se desprende de la Exposición de Motivos de la propuesta de Reglamento en materia de inteligencia artificial que, presentada por la Comisión el 21 de abril de 2021, ha sido objeto de las oportunas orientaciones generales del Consejo, de las enmiendas del Parlamento, y de otras actuaciones de órganos de la UE, hasta alcanzar el acuerdo político de los colegisladores europeos (8 de diciembre de 2023), que dio lugar al texto definitivo de 13 de junio (DOUE, 12 julio 2024). Si bien, en la propuesta inicial se definen los cuatro niveles de riesgo (sistemas prohibidos, de alto riesgo, riesgo limitado o medio y riesgo bajo) pero no se contemplan los actuales modelos de GPAI. Ver COMISIÓN EUROPEA (CE), *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206>

¹⁴ La regulación tiene como propósito la protección del ser humano, para lo que pone en valor en el considerando 27 las Directrices éticas para una IA fiable de 2019 que, elaboradas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisión Europea constituyen principios éticos -aunque no vinculantes- a tener en cuenta en el desarrollo y uso de la IA. Estos principios, no dejan lugar a dudas en cuanto a que la persona es el eje de esta regulación: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas.

Sentadas las bases de la regulación europea de la IA atendiendo al riesgo (abril de 2021), con la irrupción de *ChatGPT* (noviembre de 2022)¹⁵ se produce un tsunami tecnológico. La herramienta, de fácil acceso, gratuita y sorprendentemente resolutive y de respuesta inmediata, no deja de ser una herramienta más probabilística que certera -no busca la verdad, sino proporcionar respuestas a una velocidad impensable- que determinó que, tanto el Consejo de la Unión Europea a través de sus orientaciones generales (diciembre 2022), como el Parlamento Europeo vía enmiendas (junio 2023), también la sociedad civil, las administraciones públicas, la academia, los ciudadanos o la industria alertaran de un devenir tecnológico imparable, el de la IA generativa (IAGen, o GenAI por sus siglas en inglés) que, con infinitos beneficios e innumerables oportunidades, también presenta grandes retos y riesgos para las personas, la sociedad y la economía.

Si inicialmente la propuesta del Reglamento de IA se centraba en los sistemas de alto riesgo (tras prohibir los sistemas de riesgo inaceptable), y se ocupaba muy laxamente de los sistemas denominados «de riesgo limitado o medio», los grandes modelos de IAGen dieron muestra en pocos meses que, con sus amplias capacidades (multimodales y multifuncionales) para crear contenido aunque no estuvieran entrenados para ello, también podían vulnerar derechos fundamentales, la salud, la seguridad de las personas, las democracias, el Estado de Derecho o el medio ambiente. Si la IA está al servicio del ser humano, para proporcionarle beneficios y optimizar resultados, no cabía una regulación que dejara expuesta a la persona a los riesgos que los grandes modelos de lenguaje representan *per se*.

De ahí que esta herramienta y otros grandes modelos de IA generativa, que constituyen el ejemplo tipo de modelo de IA de uso general (considerando 99 del RIA), y que generan contenido en distintos formatos (imágenes, video, texto o audio) y cumplen distintos fines, hayan sido objeto de una regulación exhaustiva e independiente¹⁶ en el Reglamento de Inteligencia

¹⁵ En el poco tiempo que lleva de prueba, y comercialización (en versiones más actualizadas), mucho se ha escrito sobre ChatGPT y la inteligencia artificial generativa (popularizada a través de esta herramienta que realiza tareas propias de la inteligencia humana vía redes neuronales artificiales y con capacidad para supervisar su aprendizaje). Cabe citar: Muñoz García, C. (2023). «¿ChatGPT en la universidad? ¿Complementar el aprendizaje y cambiar el modelo educativo?». *Diario La Ley*, núm. 10283, marzo; Muñoz García, C. (2023) *Regulación de la inteligencia artificial en Europa. Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*. Tirant lo Blanch, Valencia, 1ª edición; Muñoz García, C. (2024) «Modelos de IA de uso general y sistemas de IA de riesgo limitado y mínimo», en *El Reglamento Europeo de Inteligencia Artificial*, dirigido por Moisés Barrio. Tirant lo Blanch, Valencia, 1ª edición. Navas Navarro, S. (2023). *ChatGPT y modelos fundacionales*. Editorial Reus, Madrid, 1.ª edición.

¹⁶ Al margen de los sistemas prohibidos (artículo 5) y de los sistemas de alto riesgo (artículo 6 y ss.), tras el capítulo IV (artículo 50), en el que se fijan obligaciones de transparencia de los provee-

Artificial (RIA), también que requieran valoración humana previa y una adecuada revisión durante todo el ciclo de vida del producto. Los potenciales riesgos exigen de normas imperativas, vinculantes, con obligaciones para el operador y requisitos técnicos rigurosos, no sólo *ex ante*, también *ex post* desde la puesta en circulación de cualquier modelo de IA. Son objeto de regulación en el capítulo V, artículos 51 a 56, si bien, el marco regulatorio no se agotará aquí, teniendo en cuenta la necesaria gobernanza y diferentes anexos que contienen requisitos obligatorios para estos modelos. A esta regulación nos referiremos más adelante.

Desde noviembre de 2022, la relevancia de los modelos ha ido *in crescendo*. No es baladí poner de relieve que en California, sede mundial de los grandes tecnológicas mundiales, el senador Scott Wiener presentó un Proyecto de ley para regular el desarrollo y uso de los modelos avanzados de IA (Ley de Innovación Segura para Modelos de Inteligencia Artificial de Frontera (*SB-1047* o *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*)¹⁷. Los avances del texto y las numerosas enmiendas a la propuesta han revelado la transcendencia de esta materia y el consenso en regularla una vez que se pretende, entre otras medidas: implementar protocolos de seguridad y protección antes de que los modelos se introduzcan en el mercado, otorgar poder al fiscal general del Estado de presentar cargos contras las empresas desarrolladoras si la herramienta representa una amenaza grave o un riesgo inminente o garantizar que un plazo breve de no más de 72 horas se informará de cualquier incidente de seguridad a un organismo competente¹⁸.

1.3. LA INCIDENCIA EN LOS DERECHOS DE LA PERSONA

Entender la IA generativa es comprender la gran dependencia de los modelos de IA con los datos de entrenamiento una vez que, se entrenan y operan con millones de datos y generan información de salida que, vía omisión o

dores y responsables del despliegue de determinados sistemas de IA -aquellos destinados a interactuar directamente con personas físicas-, un nuevo capítulo, el V, regula específicamente los modelos de IA de uso general en los artículos 51 a 56.

¹⁷ Sobre la propuesta: Danny Tobey, Ashley Carr, Karley Buckley, Kyle Kloeppel, California's (febrero 2024). SB-1047: «Understanding the Safe and Secure Innovation for Frontier Artificial Intelligence Act», *DLA PIPER*. <https://www.dlapiper.com/en/insights/publications/2024/02/californias-sb-1047>. El 29 de agosto de 2024, el Senado votó favorablemente (29 frente a 9), el proyecto de ley de seguridad de la IA. Finalmente, a falta de la aprobación definitiva, el veto, el gobernador de California, Gavin Newsom ha rechazado la tan ansiada regulación de las obligaciones para empresas que promuevan o desarrollen modelos de IA.

¹⁸ Con todo, son muchas las críticas que ha recibido el texto por entender que el marco regulatorio excesivamente imperativo y sancionador es una amenaza para el progreso de la IA, y una consecuente salida del Estado de California de empresas tecnológicas e ingenieros.

acción- puede dañar múltiples derechos de las personas. Por lo que los retos éticos y legales son incuestionables. De ahí que, ser riguroso desde el diseño y evaluar los posibles daños, ayudará a evitar o minimizar los riesgos para que los modelos y sistemas no socaven estos derechos. Por lo pronto, la normativa europea impone obligaciones al operador, requisitos técnicos rigurosos, y sistemas de control post puesta en circulación del modelo en el mercado europeo.

2. TAXONOMÍA DE LOS MODELOS DE IA DE USO GENERAL

2.1. DEFINICIONES LEGALES Y CLASIFICACIÓN

Según el tenor literal del artículo 3 del RIA, son muy numerosas las definiciones que ayudaran a entender lo disruptivo de esta tecnología. Todas ellas son esenciales a los efectos del Reglamento. Pues bien, alejada en el texto definitivo de la primera de las definiciones sobre lo que se entiende por «sistema de IA»¹⁹, el legislador europeo nos proporciona, entre los últimos apartados del citado artículo 3, en los apartados 63 y 65, qué se entiende a los efectos del Reglamento por «modelos de IA de uso general» y qué son los «sistemas de IA de uso general». Visualizar ambos conceptos ayudará a entender la importancia de lo primero y cómo estos son la base de los segundos:

(63) «Modelo de IA de uso general: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando auto supervisión a gran escala, que presenta un grado considerable de generalidad significativa y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado».

¹⁹ La definición de «sistema de IA» proporcionada por el RIA es la primera con la que se inicia el artículo 3 (disposiciones generales): «*un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*». Esta, alineada con la proporcionada por la OCDE en noviembre de 2023 (tras la revisión a la inicialmente dada en 2019), da cumplida muestra del consenso que existe entre la UE y la OCDE en proporcionar una definición amplia, flexible, y que se adapte a los sucesivos cambios tecnológicos.

(66) «Sistema de IA de uso general: un sistema de IA basado en un modelo de IA de uso general y que puede servir a diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA».

Con lo dicho en la última de las definiciones, queda claro la dependencia de la segunda respecto de los modelos de IA. Veremos también, cómo los modelos pueden también incorporarse a otros sistemas de IA de mayor riesgo, lo que no eximirá de obligaciones ni a quien proporciona el modelo, ni a quien lo integra en su sistema.

Ahora bien, dicho lo anterior, la herramienta se incorpora a sistemas de IA, en su mayoría a los de riesgo medio o limitado, como son los chatbots conversacionales que tanto han proliferado desde la aparición de ChatGPT y que muestran habilidades extraordinarias pero que también hacen difícil distinguir cuando responde un humano y cuando responde una máquina²⁰. No olvidemos que la inteligencia artificial generativa (popularizada a través de esta herramienta que realiza tareas propias de la inteligencia humana opera vía redes neuronales artificiales y con capacidad para supervisar su aprendizaje).

Partiendo de todo lo anterior habrá modelos de IA de uso general que lo serán «con riesgo sistémico», y por tanto, con obligaciones más rigurosas para los proveedores de la herramienta y sujetos a mayores requisitos técnicos, ¿qué modelos son estos?

- (1) Aquellos que tienen *capacidades de gran impacto*, según el artículo 3, apartado 64), evaluadas conforme a parámetros actualmente fijados en el artículo 51, apartado 2 de RIA. Y es así *cuando la cantidad acumulada de cálculo utilizada para su entrenamiento medida en operaciones de coma flotante, sea superior a 10^{25}* ;
- (2) y además, presentan *un riesgo específico con repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor del modelo de IA*, como expresa el artículo 3, apartado 65).

²⁰ Con TURIN, A.M. (1950). «Computing Machinery and Intelligence». *Mind* 49: 433-460, a través del test de Turing se planteó: «¿Pueden pensar las máquinas?». Para responder a esta cuestión entra en juego el concepto de la máquina pensante y se plantea si es posible que algún día puede llegar a reproducir el pensamiento humano, admitiendo en aquel entonces que, era muy probable que las máquinas estén en condiciones de competir con los hombres en todos los aspectos intelectuales. Hoy aquellos planteamiento se consideran que sientan las bases de la denominada inteligencia artificial. Visto en <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>

2.2. LA EXIGENCIA GENERAL DE TRANSPARENCIA Y UNA REGULACIÓN SINGULAR PARA LOS MODELOS DE GPAI

Con carácter previo, es oportuno precisar que, en concurrencia con lo anterior, en el capítulo IV, y en un único precepto, bajo un mismo título (*obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA*), el artículo 50, dejando al margen aquellos sistemas que, no son los prohibidos por el riesgo o la amenaza inaceptable que representan (artículo 5 del RIA), ni los de alto riesgo, sujetos a obligaciones, requisitos y controles muy rigurosos (artículo 6 y ss. del RIA), busca garantizar la máxima transparencia en la herramienta objeto de este capítulo. De forma que, aquellos sistemas destinados a interactuar con personas físicas -o generen contenido sintético-, deben ser diseñados y desarrollados de manera que estos sujetos sepan que interactúan con un sistema de IA, lo que no excluye determinadas excepciones. De ahí, la exigencia de transparencia tanto para los modelos de IA de uso general como para los sistemas de IA de uso general (artículo 3, apartados 63 y 66 del RIA).

A los efectos, reitero lo ya dicho con anterioridad, si de base los modelos de inteligencia artificial generativa (IAGen) son ejemplo tipo de los modelos de GPAI («general-purpose AI models/systems» según el RIA), principalmente por su capacidad para crear contenido multimodal y servir a diversos fines, no es menos cierto que para todos ellos es necesario establecer medidas de información y transparencia proporcionadas a los riesgos que generan²¹.

En términos generales, ¿cuándo estamos ante un modelo de IA de uso general?²² De partida, del considerando 97 y del artículo 3, apartado 63) del RIA podemos extraer algunas ideas principales sobre los modelos de IA de uso general (modelos de GPAI o *GPAI model*):

- No constituyen por sí mismos sistemas de IA;
- La definición contiene las características funcionales esenciales que son la generalidad y la capacidad para realizar una amplia gama de tareas diferenciadas;
- Pueden introducirse en el mercado y comercializarse en diversas formas (a través de bibliotecas, interfaces de programación de aplicaciones -API-, como descarga directa o como copia física), si bien,

²¹ Muñoz García, C. «Artículo 51 del Reglamento de Inteligencia Artificial», en Barrio Andrés, M., (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, Editorial La Ley, Madrid, 2024.

²² En Muñoz García, C. «Artículo 53 del Reglamento de Inteligencia Artificial» y «Artículo 55 del Reglamento de Inteligencia Artificial», en Barrio Andrés, M., (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, Editorial La Ley, Madrid, 2024.

para entonces, ya deben cumplirse las obligaciones y requisitos técnicos exigidos en el RIA;

- Pueden modificarse, perfeccionarse y transformarse en nuevos modelos.
- Además, el Reglamento clasifica esta herramienta en función de sus capacidades y riesgos: (i) si no superan determinados umbrales tendrán encaje como modelos de IA de uso general -sin más-, por lo que, para diferenciarlos de los siguientes los he denominado modelos de GPAI «simple» (así los he denominado en otras publicaciones)²³; (ii) o bien, si la herramienta supera determinados umbrales se clasificará como modelo «con riesgo sistémico» (como denomina el legislador europeo a los que, sin ser sistemas de «alto riesgo», están más próximo a este).

El capítulo V al que dedica este apartado y que incluye seis artículos es un epígrafe singular incorporado tras la irrupción de ChatGPT (noviembre de 2022), tras un largo proceso de estudio, debates y negociaciones sucesivas operadas a partir de las enmiendas del Parlamento (junio de 2023) y como resultado del acuerdo político alcanzado por los colegisladores europeos (diciembre de 2023), da muestra de la relevancia de estos modelos grandes de lenguaje que emulan la inteligencia humana.

Los 6 preceptos que lo conforman están distribuidos en cuatro secciones, lo que en mi opinión, proporciona unos contenidos específicos y muy bien delimitados²⁴. En todos ellos, el punto de partida es la diferenciación de los modelos de IA de uso general de los modelos de IA de uso general «con riesgo sistémico». Para estos últimos, definidos por su altas capacidades e impacto negativo en el mercado, y que representa una mayor probabilidad de riesgos para derechos protegidos -a diferencia de un modelo de «GPAI simple»-, la regulación prevé normas específicas propias que se adicionan a las obligaciones y requisitos de los modelos carentes de riesgo sistémico.

²³ En Muñoz García, C. «Artículo 51 del Reglamento de Inteligencia Artificial», en Barrio Andrés, M, (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, Editorial La Ley, Madrid, 2024; También en Muñoz GARCÍA, C. *Regulación de la inteligencia artificial en Europa. Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*. Editorial Tirant lo Blanch, 2023. Valencia, 1.^a edición.

²⁴ Para un análisis más detallado, ver Muñoz García, C. «Artículo 51 del Reglamento de Inteligencia Artificial», «Artículo 52 del Reglamento de Inteligencia Artificial», «Artículo 53 del Reglamento de Inteligencia Artificial» «Artículo 53 del Reglamento de Inteligencia Artificial», «Artículo 54 del Reglamento de Inteligencia Artificial», «Artículo 55 del Reglamento de Inteligencia Artificial», y «Artículo 56 del Reglamento de Inteligencia Artificial», en Barrio Andrés, M, (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, Editorial La Ley, Madrid, 2024 (disponible en octubre de 2024).

Con todo, junto a este capítulo singular para estos modelos (aspectos sustantivos), el RIA alberga anexos -XI, XII y XIII- referidos a esta herramienta (aspectos técnicos) y otros artículos fuera del capítulo V. A unos y otros nos referiremos de manera breve para dar el enfoque necesario al objeto de conocer los riesgos que estas herramientas puedan generar.

2.3. MARCO REGULATORIO PROPIO

De manera sucinta podríamos proceder a seguir la clasificación que sigue el capítulo V del RIA, y que se divide en cuatro secciones, incluyendo un total de seis artículos sobre los dos modelos de IA de uso general. Esta regulación proporciona un margo regulatorio singular dirigido a que esta herramienta, cada vez más común, cumpla una serie de requisitos y se comercialice en la UE con las máximas garantías. Así lo hemos hecho con ocasión de otras publicaciones precedentes²⁵. Sin embargo, el afán de plantear una taxonomía de los modelos de IA de uso general para abordar la naturaleza de esta herramienta que puede llegar a presentar un riesgo sistémico y que puede variar su capacidad e incluso integrarse en sistemas de alto riesgo o prohibidos, nos ayudará a identificar los riesgos en el mercado de la Unión y a proveer de alertas y medidas eficaces que minimicen los riesgos.

2.3.1. Obligaciones y requisitos técnicos para los modelos de IA de uso general o «GPAI simple»

Cómo hemos advertido con anterioridad, no estamos ante sistemas, no tienen grandes capacidades, pero están sujetos a modificaciones y cambios que pueden alterar su denominación como modelos de IA de uso general simple, o integrarse en sistemas que supongan un alto riesgo, o incluso, en sistemas prohibidos. Para estos modelos, de inicio, que se contemplan en la sección segunda, bajo el título de *obligaciones de los proveedores de modelos de IA de uso general*, dos artículos.

- (i) Artículo 53. Obligaciones de los proveedores de modelos de IA de uso general

Al margen de modelos de GPAI con riesgo sistémico, el artículo 53 precisa cuáles son las obligaciones para todo proveedor con independencia del mo-

²⁵ Muñoz García, C. *Comentarios...* op. cit. ant. y en «Modelos de IA de uso general y sistemas de IA de riesgo limitado y mínimo», en *El Reglamento Europeo de Inteligencia Artificial*, op. cit. ant.

delo que incorpore o comercialice en el mercado de la Unión. En este caso se fijan, con carácter imperativo y de generalidad, las siguientes obligaciones:

- a) Elaboración y mantenimiento actualizado de la documentación técnica del modelo, incluida la información relativa al proceso de entrenamiento, pruebas y evaluación, en los términos del anexo XI. La misma, deberá estar disponible, por si le fuese solicitada, por la Oficina Europea de IA y de las autoridades nacionales competentes que así la soliciten (artículo 53, apartado 1, letra a).
- b) Además, deberá poner la documentación a disposición del proveedor posterior de sistemas de IA que tenga la intención de integrar el modelo de IA de uso general en sus sistemas de IA, de manera clara y comprensible, de modo que les permita conocer las capacidades y limitaciones (artículo 53, apartado 1, letra b). Y ello sin perjuicio de la expresa obligación de informar y cumplir la legislación vigente en materia de propiedad intelectual e industrial, información empresarial confidencial o los secretos comerciales de conformidad con el Derecho europeo y nacional (artículo 53, apartado 1, letra c).
- a) En todo caso, establecerán directrices para cumplir la normativa europea en materia de derechos de autor y, derechos afines, y más concretamente, para identificar y salvaguardar la reserva de derechos de autor prevista en el artículo 4, apartado 3, de la Directiva 2019/790. Téngase en cuenta que, todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras y otras prestaciones con fines de prospección de textos y datos en determinadas circunstancias (considerando 106).
- b) Además, deberá elaborar y poner a disposición de los usuarios finales un resumen suficientemente detallado del contenido utilizado para el oportuno entrenamiento, según modelo habilitado para ello por la Oficina de IA (artículo 53, apartado 1, letra d).

Dicho esto, es pertinente precisar que quedan al margen de estas obligaciones los proveedores de modelos de GPAI «simple» que se divulguen conforme a una licencia libre y de código abierto, que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Sin

embargo, dicha excepción no cabe cuando estemos ante modelos «con riesgo sistémico» (artículo 53, apartado 2), o media cualquier tipo de contraprestación o monetización del modelo (considerando 103).

(ii) Artículo 54. Representantes autorizados de los proveedores de modelos de IA de uso general

A las anteriores obligaciones se suma que, cuando se trata de un proveedor de un tercer país ajeno a la Unión que pretende introducir un modelo de IA de uso general, este tiene el deber previo de designar un representante autorizado. Uno y otro, proveedor y representante autorizado son tratados en pie de igualdad en el Reglamento a efectos de la aplicación de la norma. Es una exigencia incuestionable para introducir un modelos de IA en el mercado de la UE.

No parece difícil interpretar este artículo en el sentido de que exige, de manera expresa, el nombramiento de un responsable autorizado cuyo mandato le encomienda realizar las tareas previstas en el citado artículo. Es obvio que, debe estar debidamente informado sobre el sistema o modelo de IA que pretende introducir en el mercado y que sabe lo que ello representa. Téngase en cuenta que sobre él recae el foco de cualquier actuación que se solicite por las instituciones europeas y nacionales competentes. Es él quien debe facilitar a las autoridades toda la información necesaria sobre el modelo, proporcionar la documentación y probar que este cumple tanto obligaciones como requisitos técnicos fijados para cualquier modelo de IA de uso general. En definitiva, el representante autorizado debe estar en condiciones de rendir cuentas cuando sea requerido²⁶.

(iii) Requisitos técnicos de los anexos XI y XII del RIA

En términos generales, y para todos los modelos de GPAI, sin distinción, es preciso cumplir requisitos técnicos y cumplimentar documentación con información clara y precisa. En este sentido, el antepenúltimo y penúltimo anexo del Reglamento, precisan cuál es esta documentación, según que medie o no un proveedor posterior²⁷:

²⁶ Así lo hemos expresando en «Artículo 54 del Reglamento de Inteligencia Artificial», en Barrio Andrés, M., (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, Editorial La Ley, Madrid, 2024 (disponible en octubre de 2024).

²⁷ En el artículo 3, apartado 68), última de las definiciones que nos proporciona el RIA, es «proveedor posterior»: *un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales.*

- Anexo XI, «Documentación técnica a que se refiere el artículo 53, apartado 1, letra a) -documentación técnica para proveedores de modelos de IA de uso general». Sobre esta documentación, cabe precisar dos aspectos: el primero, la exigencia general contenida en este anexo, concretamente lo contenido en la sección primera, que es aplicable a cualquier proveedor de estos modelos de GPAI, ya sean «simples» o «con riesgo sistémico». Y es así porque lo contenido en la sección segunda, con requisitos técnicos, y exigencias adicionales, sólo es aplicable para los modelos «con riesgo sistémico»; el segundo aspecto a precisar es que, dicha documentación técnica, al igual que ocurre con la incluida en los siguientes anexos, debe estar a disposición de la Oficina de IA y de las autoridades nacionales que tengan competencias en la materia;
- Anexo XII «Información sobre transparencia a que se refiere el artículo 53, apartado 1, letra b) -documentación técnica de los proveedores de modelos de IA de uso general para los proveedores posteriores que integren el modelo en su sistema de IA», y que deberá albergar un mínimo de información (además de una descripción general del modelo, deberá contener una descripción más detallada de los elementos del modelo y de su proceso de desarrollo, incluidos otros requisitos). Esta documentación e información debe ser proporcionada por el «proveedor» inicial (artículo 3, apartado 3) al «proveedor posterior» (artículo 3, apartado 68).

2.3.2. Obligaciones y requisitos técnicos para los modelos de IA de uso general «con riesgo sistémico»

En la sección primera se incluyen dos artículos sobre *reglas de clasificación*, ambos dirigidos a clasificar un modelo de IA en la categoría prevista como herramienta con riesgo sistémico. Para ello, el legislador europeo determina cuándo se denominará como tal y fijará el procedimiento para hacerlo:

- (i) Artículo 51. Reglas de clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgo sistémico.

En este artículo, partiendo de la definición genérica de modelos de IA de uso general (artículo 3, apartado 63 del RIA), y teniendo en cuenta que las ca-

pacidades de gran impacto de la herramienta (artículo 3, apartado 64 del RIA)²⁸ inciden en su clasificación como «Modelos de IA de uso general con riesgo sistémico» (artículo 3, apartado 65 del RIA)²⁹, estaremos alerta respecto a determinados modelos. Así, esta singular denominación, conforme este último párrafo 65 del artículo 3 (definiciones), se asocia a un criterio objetivo: (i) para los modelos con capacidades de alto impacto *evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia*, (ii) y además, cuyas capacidades producen un impacto considerable en el mercado interior *debido a su alcance, o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto*.

La denominación como modelos con riesgo sistémico determinará un régimen regulatorio más severo en cuanto a obligaciones y requisitos técnicos de la herramienta.

Ahora bien, a la denominación como modelos con riesgo sistémico se puede llegar por dos vías: una primera, vía presunción *iuris tantum*, en cuanto admite prueba en contrario, y una segunda vía imposición de la Comisión. En el primer supuesto se tratará de un modelo de GPAI con capacidades de alto impacto *cuando la cantidad acumulada de cálculo utilizada para su entrenamiento medida en operaciones en coma flotante sea superior a 10^{25}* (artículo 51, apartado 1, letra a), mediante el criterio objetivo señalado anteriormente; en el segundo, dicha denominación deriva de la potestad reconocida a la Comisión para reevaluar y calificar, de oficio o con ocasión de una alerta cualificada por parte del grupo de expertos científicos, un modelo de uso general simple en modelo de uso general de riesgo sistémico. Es más, en base a esta potestad la Comisión adoptará actos delegados conforme artículo 97 para reevaluar y actualizar los umbrales y criterios fijados en el artículo 51 con arreglo a los criterios fijados anexo XIII.

(ii) Artículo 52. Procedimiento.

Es inevitable que, cuando un modelo de GPAI cumpla el requisito objetivo al que se refiere el artículo 51, apartado 1, letra a) -en cuanto a tener *capa-*

²⁸ El Reglamento determina cuándo los modelos de IA se consideran herramientas con riesgo sistémico cuando estas «capacidades de gran impacto: capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados» (artículo 3, apartado 64 del RIA).

²⁹ En el Reglamento se califica como modelo con «Riesgo sistémico», cuando se da «un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor».

ciudades de gran impacto, o un impacto equivalente teniendo en cuenta los criterios establecidos en el anexo XIII-, el proveedor deba comunicarlo. Así, se fija la obligación de notificar a la Comisión «sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse», que ha superado el umbral previsto o que va a superarlo. Esto determina, de primeras, la presunción de que el modelo debe soportar una nueva denominación, la de modelo «con riesgo sistémico».

Si no media notificación por el proveedor, la Comisión podrá decidir la calificación del modelo como de «riesgo sistémico», y además, podrá exigir el cumplimiento de las obligaciones impuestas en el Reglamento a los proveedores de modelos de IA de uso general mediante varias medidas, entre otras, la imposición de multas administrativas.

¿Puede escapar el proveedor de una calificación que le sujeta a mayor número de obligaciones? El proveedor de esta herramienta, obligado a notificar y documentar las capacidades de gran impacto del modelo, también intentará justificar que dichas habilidades, aun cuando superan el umbral aplicable, o está próximo a cumplirse este (artículo 52, apartado 2, en relación con el artículo 51, apartado 1, letra a) y artículo 51, apartado 2), no presenta riesgos sistémicos (artículo 52, apartado 2). Con todo, la decisión última corresponde a la Comisión, que es de quien depende la nueva calificación.

(iii) Artículo 55. Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico.

La sección tercera incluye un único artículo para regular los modelos de GPAI con riesgo sistémico. Por un lado, en el primer párrafo del artículo 55, párrafo 1º, nos remite a las obligaciones fijadas para cualquier modelo de GPAI al artículo 53³⁰, por lo que las obligaciones de documentación e información deberán ser también cumplidas por los proveedores de modelos de GPAI «con riesgo sistémico». Además, se añaden otras obligaciones adicionales, conforme precisa el mismo artículo 55, párrafo 1 del RIA:

- a) Realizar evaluación del modelo conforme protocolos y herramientas normalizados, lo que conlleva documentar que se han llevado a efecto pruebas de simulación de adversarios, al objeto de reducir los riesgos sistémicos posibles.
- b) Evaluar y adoptar las medidas necesarias para reducir los posibles riesgos sistémicos que puedan producirse por el desarrollo, introducción o uso del modelo en el mercado interior.

³⁰ Aplicable a cualquier modelo, con independencia de las capacidades y riesgos que genera.

- c) Hacer un seguimiento, documentar y notificar incidentes graves y las medidas correctoras para solventarlo, tanto a la Oficina de IA como a la autoridad nacional que sea competente. En definitiva, estar vigilantes y notificar sin demora incidentes graves.
- d) Adoptar las medidas necesarias para garantizar la óptima protección de la ciberseguridad del modelo.

(iv) Requisitos técnicos del anexo XIII del RIA

A todos las obligaciones de los modelos de IA de uso general, se han sumado las propias de esta herramienta que presenta riesgo sistémico. Y lo mismo ocurre respecto a los requisitos técnicos fijados para estos modelos. Así, en el último anexo del Reglamento, se suman criterios específicos fijados en los comunes de los anexos XI y XII (este último del proveedor inicial al proveedor posterior):

· Anexo XIII «Criterios para la clasificación de los modelos de IA de uso general con riesgo sistémico a que se refiere el artículo 51». Y es así con el propósito de determinar si un modelo tiene capacidades de gran impacto o un impacto equivalente a los fijados en el artículo 51, apartado 1, letra a) del RIA. Para esta calificación, la Comisión tendrá en cuenta (y transcribo, casi literalmente, los criterios o indicadores que incluye el citado anexo):

- a. Número de parámetros del modelo;
- b. Calidad o tamaño del conjunto de datos empleados, medido, por ejemplo a través de criptofichas;
- c. La cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para dicho entrenamiento;
- d. Modalidades de entrada y salida del modelo, ya sea en igual modalidad o multimodal (por ejemplo, de texto a imagen) y los umbrales del estado de la técnica para determinar las capacidades de alto impacto para cada modalidad, y el tipo específico de entradas y salidas (por ejemplo, secuencias biológicas);
- e. Parámetros de referencia y evaluaciones de las capacidades del modelo, también considerando el número de tareas sin formación adicional, la adaptabilidad para aprender tareas nuevas y distintas, su grado de autonomía y escalabilidad, las herramientas a las que tiene acceso;

- f. El impacto en el mercado interno teniendo en cuenta su alcance. Para lo que se fija como parámetro que el modelo se haya puesto a disposición de al menos 10.000 usuarios profesionales registrados en la UE;
- g. Número de usuarios finales registrados.

Estos, al margen de los requisitos técnicos comunes forman parte del proceso de diseño y desarrollo de cualquier modelo de IA, en cuanto la documentación e información clara y transparente que debe acompañarse contiene todos los parámetros e indicadores que ayudaran a comprender la capacidad del modelo y los potenciales riesgos que genera.

2.3.3. Los códigos de buenas prácticas

El artículo 56 del Reglamento, último del capítulo VI, en la cuarta y última sección³¹, al objeto de facilitar el cumplimiento y homogeneización de las obligaciones a cumplir por el proveedor de esta herramienta, ya se de un modelo de GPAI simple, ya lo sea con riesgo sistémico, propicia la creación de los *códigos de buenas prácticas* para ayudar a implementar y cumplir los deberes y requisitos exigidos por la norma.

Constituye una herramienta esencial para el cumplimiento de las obligaciones fijadas en los artículos precedentes y dada su relevancia, la Comisión, mediante actos de ejecución, podrá aprobar un código de buenas prácticas y otorgarles una validez general en la UE (considerando 117 del RIA)³².

Cualquier proveedor de modelos de IA de uso general, independientemente del riesgo que conlleva, podrá valerse de códigos de buenas prácticas en los términos del artículo 56. Esta práctica, y a falta de una norma armonizada europea, favorece a quien la lleve a efecto en cuanto supone la presunción de cumplimiento de las obligaciones a las que obliga el Reglamento según el modelo de que se trate, ya sean las contenidas en el artículo 53 apartado 1 o en el artículo 55 del Reglamento.

³¹ Muñoz García, C. «Artículo 56 del Reglamento de Inteligencia Artificial», Barrio Andrés, M, (coord.), *Comentarios al Reglamento de Inteligencia Artificial*, op. cit.

³² Por la Comisión Europea se ha abierto un período de consulta al objeto de elaborar un Código de buenas prácticas que comprenda las obligaciones específicas contenidas en el Reglamento para estos modelos. El período de consultas se llevará a efecto con el propósito de establecer las reglas relacionadas con la transparencia exigida, el cumplimiento de las obligaciones del capítulo V del RIA, de los derechos de autor y afines, la identificación de los riesgos y medidas de evaluación para riesgos sistémicos, también medidas de mitigación de los mismos y políticas y gestión interna de riesgos y gobernanza. Sobre la consulta <https://artificialintelligenceact.eu/es/introduction-to-codes-of-practice/>

Por lo pronto, el proveedor tiene la potestad de adherirse a códigos de buenas prácticas que, vaya por delante, deben comprender, al menos, las obligaciones establecidas en el artículo 53 y 55, según el modelo de IA de uso general de que se trate. El cumplimiento de estas obligaciones es incuestionable, por una vía u otra, al fin y a la postre se consideran una herramienta fundamental para el cumplimiento de las obligaciones impuestas en el RIA y deberá reflejar fielmente que cumple con los propósitos de la norma.

Con todo, el artículo 53, apartado 4 (para los modelos de IA de uso general simple), y el artículo 55, apartado 2 (para los modelos con riesgo sistémico), remiten al artículo 56 del RIA y ofrecen otras alternativas al proveedor, en cuanto le cabe probar que cumple las obligaciones por otros medios idóneos que se someterán a evaluación de la Comisión.

Si el marco regulatorio de los modelos de GPAI se aplicará al año de la entrada en vigor del RIA, en agosto de 2025, el Código de Buenas Prácticas estará finalizado a más tardar el 2 de mayo de 2025 (artículo 56, apartado 9 del RIA). Normas comunes para adoptar unas obligaciones homogeneizadas en el texto.

2.3.4. Otros preceptos a tener en cuenta

La anterior regulación especial contenida en el capítulo V, artículos 51 a 56, no agota todas las obligaciones para estos proveedores. Estos modelos están sujetos a mantener la coherencia en los términos del RIA durante todo el ciclo de vida de la herramienta y estarán bajo supervisión, por lo que también le son de aplicación, principalmente, los siguientes preceptos:

- En el capítulo IX sobre «Vigilancia poscomercialización, intercambio de información y vigilancia del mercado», la concreta sección 3 (artículos 74 a 84), sobre «garantías del cumplimiento» incluye el deber de confidencialidad de cualquier persona física o jurídica que participe en la aplicación del RIA. Por otro lado, en la sección 5 (artículos 88 a 94), estos últimos artículos se ocupan específicamente de la «supervisión, investigación, cumplimiento y seguimiento respecto de proveedores de modelos de IA de uso general»;
- Capítulo X, titulado «Códigos de conducta y directrices». Se admite que, la Oficina europea de IA y los EE.MM. fomentarán y facilitarán la elaboración de códigos de conducta, con sus correspondientes mecanismos de gobernanza, para la aplicación voluntaria de requisitos específicos (artículo 95). El propósito es claro, que aún cuando no estemos ante sistemas de alto riesgo, conviene que, voluntaria-

mente, los proveedores de sistemas de IA de menor riesgo, incluidos los sistemas de IA de uso general –basado en un modelo de IA de uso general-, apliquen los requisitos del capítulo III, sección 2 (artículos 8 a 15), en aras de llevar a efecto las mejores prácticas del sector;

- Capítulo XII. «Sanciones». Se atribuye a los Estados miembros el régimen de sanciones y otras medidas de ejecución, como advertencias o medidas no pecuniarias, aplicable a los operadores que infrinjan el RIA (artículo 99 de dicha norma). Ahora bien, los EE.MM. darán cuenta a la Comisión, a más tardar en la fecha de la aplicación de las sanciones (a los veinticuatro meses de la entrada en vigor del RIA), de sus normas internas referentes a las sanciones y otras medidas de ejecución mencionadas en el artículo 99 del RIA. Por otro lado, será el artículo 101 del texto el que se ocupe de las multas a proveedores de modelos de IA de uso general, que habrán de ser efectivas, proporcionadas y disuasorias. Lo singular es, que en este caso, corresponde a la Comisión imponer las multas administrativas³³, cuando considere que el proveedor ha infringido el Reglamento de forma deliberada o negligente³⁴.

3. EL RIESGO EN LOS MODELOS Y SISTEMAS GPAI ¿CRITERIO SUFICIENTE PARA FIJAR LA OBJETIVACIÓN DE LA RC?

El enfoque del Reglamento de Inteligencia Artificial con fundamento en el riesgo de esta tecnología para la salud, la seguridad, y los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, es la base de la clasificación de los sistemas de IA y de los modelos de GPAI. Y en consecuencia, la razón de ser para crear normas imperativas, vinculantes y proporcionadas a la contingencia probable que menoscabe cualquiera de los derechos protegidos por el acervo de la Unión.

A mayores riesgos de los sistemas y modelos de IA, también de los productos y servicios conexos de la IA que puedan afectar principalmente a la intimidad, la protección de datos, los derechos de los consumidores, a derechos

³³ El incumplimiento de las disposiciones del Reglamento por el proveedor puede dar lugar a multas administrativas de hasta el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15.000.000 EUR, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia, el proveedor del modelo infringió alguna de las obligaciones fijadas en el Reglamento (artículo 101 RIA).

³⁴ Lo que no es obstáculo para exigir por el perjudicado la pertinente responsabilidad por daños.

fundamentales, el empleo, la protección de los trabajadores y seguridad de los productos, entre otros³⁵, mayores requisitos técnicos y obligaciones, mayor control post comercialización, reglas más rigurosas de gobernanza y sanciones más elevadas.

Si los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general³⁶, cabe plantearse si modelos como GPT son útiles como caso de uso para acercarnos a los riesgos probables de la herramienta y a la hipotética responsabilidad por daños a terceros. A modo meramente de ejemplo cabe citar, entre otros probables perjuicios, los siguientes: el uso malicioso en sectores críticos (la salud, la movilidad, el empleo o la energía), la elaboración de perfiles, la suplantación, la desinformación, el fraude, la discriminación, la infracción de los derechos de autor, o la injerencia en la privacidad o protección de datos.

El *Monitor de incidentes de IA de la OCDE* publicado por el grupo de expertos de la OCDE. AI sobre incidentes de la IA en mayo de 2025 nos ayudará a identificar y dar visibilidad a estos riesgos que pueden menoscabar derechos plenamente consolidados en el Derecho de la Unión³⁷.

Por otro lado, el *Convenio Marco del Consejo de Europa sobre Inteligencia Artificial*³⁸, tras admitir que es prioritario fijar un marco jurídico aplicable a nivel mundial, y de fijar como objetivos proteger los derechos humanos, la democracia y el Estado de Derecho, expresa que la IA, en todo su ciclo de vida, se enfrenta a retos y riesgos de hondo calado. Entre otros, cita que los sistemas

³⁵ En estos términos se expresa el considerando 9 del Reglamento.

³⁶ Considerando 99 del RIA.

³⁷ La OCDE presentó en mayo de 2024 *Monitor de incidentes de IA de la OCDE* sobre la importancia de la Metodología y divulgaciones de daños reales y probables del desarrollo y uso de la IA, no sin antes advertir que este paper se elabora tras monitorear noticias mundiales y que estos perjuicios, muy probablemente, sólo representen un subconjunto de todos los incidentes y peligros de IA en el mundo <https://oecd.ai/en/incidents-methodology>

³⁸ El *Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Recursos Humanos Derechos, democracia y Estado de Derecho* (CETS - No. 225), aprobado en mayo, y publicado para firmas de adhesión el 05.09.2024, tras reconocer en el preámbulo el valor y el potencial en beneficio humano de la IA y que pretende alcanzar la unidad en el tratamiento de esta tecnología y la cooperación con terceros Estados que comparten los mismos valores, admite cuáles son muchos de los riesgos de la IA. Si se trata de promover y proteger los derechos humanos, el bienestar individual y social, el desarrollo sostenible, la igualdad de género, y el empoderamiento de todas las mujeres y niñas, así como otros objetivos e intereses importantes, potenciando el progreso y la innovación, admite que las oportunidades que proporciona la IA para la vida de las personas conlleva grandes retos y riesgos para garantizar los derechos humanos, la democracia y el Estado de Derecho <https://rm.coe.int/1680afae3c>. Mención especial merece el análisis comparativo entre el RIA y el Convenio Marco del Consejo de Europa realizado por Dignum, V. (Umeå universitet, Suecia, académica, experta en Ciencias computacionales y directora del *AI Policy Lab*), sobre «How Europe is shaping AI for human rights» en *AI Policy Lab*, (5.09.2024). Visto en <https://aipolicylab.se/2024/09/05/how-europe-is-shaping-ai-for-human-rights/>

de IA *pueden socavar la dignidad humana y la autonomía individual*³⁹, los derechos humanos, la democracia y el Estado de Derecho; generan riesgos de discriminación en contextos digitales, particularmente aquellos que involucran sistemas de inteligencia artificial y su efecto potencial de crear o agravar desigualdades, incluidas las vividas por mujeres y personas en situación de vulnerabilidad, en cuanto a los derechos humanos y en cuanto a su participación plena en condiciones de igualdad en la vida económica, asuntos sociales, culturales y políticos; que *se usen con fines represivos en violación del derecho internacional de los derechos humanos, incluso mediante prácticas de vigilancia y censura arbitrarias o ilegales que erosionan la privacidad y la integridad personal*. Va más allá cuando admite que también la tecnología tiene un gran impacto en *la salud humana, el medio ambiente o en los aspectos socioeconómicos como el empleo y la mano de obra*.

Sin duda, todo un conjunto de riesgos que habrá que mitigar mediante una regulación rigurosa y una gobernanza eficiente. En todo caso, no deja de aludirse en cualquiera de los textos que todo gira en torno a la persona, titular de derechos, y para esta se exigen, entre otros: la necesaria transparencia de la IA al en el artículo 8 del Convenio al determinar que es imprescindible en cualquier actividad del ciclo de vida de los sistemas, que en la herramienta la persona pueda identificar cuándo los contenidos son generados por sistemas de IA. También, en el artículo 9 alude a la necesidad de garantizar la rendición de cuentas y responsabilidad.

Con lo antedicho, si todo gira en torno a la persona física, sujeto de derechos, y dado que el ser humano está en el enfoque regulatorio en cualquiera de estos y otros marcos jurídicos propuestos, hay que poner en valor que junto al objetivo de proteger a la persona, hay que identificar los riesgos a los que la nueva tecnología expone a la persona. De ahí que, resulte completamente oportuno que el RIA -hito en gobernanza de la IA- adopte el enfoque basado en el riesgo que conlleva esta tecnología, y la regule atendiendo a la probabilidad de perjuicios para garantizar el cumplimiento del Derecho en su conjunto. Lo que implica que, a mayores riesgos, más obligaciones y requisitos, una supervisión más estricta para evitar o mitigar los riesgos que la tecnología con ella, y una gobernanza más rigurosa.

³⁹ Así se precisa en el artículo 7 del Convenio Marco, y en iguales términos en el considerando 27 del RIA cuando afirma que, al igual que en las Directrices éticas para una IA fiable, elaboradas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisión, hay siete principios éticos no vinculantes para la IA pero que sirven para garantizar la fiabilidad y el fundamento ético de la IA. Sobre el primero de ellos, la «acción y supervisión humanas», se pretende que los sistemas de IA se desarrollen y utilicen como *herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funcione de manera que pueda ser controlada y vigilada adecuadamente por seres humanos*. Según el considerando 27 del RIA, también servirá este principio, junto con otros seis, para la elaboración de códigos de conducta que acerquen al cumplimiento del marco regulatorio de la Unión.

Lo anterior, en mi opinión, debería haberse trasladado a normativas como la de responsabilidad por daños causados por IA, y por el momento, nada más lejos de la realidad. El enfoque del riesgo en los sistemas de IA en poco o nada se ha tenido en consideración para propiciar la responsabilidad extracontractual por daños causados por la IA. Así es que mientras en la responsabilidad por producto (que incluye también el *software*) rige la responsabilidad objetiva, en la responsabilidad por daños causados por la IA, se parte de una necesaria conducta culposa, que si bien cuenta con presunciones refutables, se aleja de los modelos de responsabilidad objetiva⁴⁰.

3.1. DEFINICIONES SOBRE EL RIESGO. IDENTIFICAR INCIDENTE Y PELIGRO DE IA

Es relevante tener en cuenta el concepto que del riesgo aporta el Reglamento en el artículo 3. En este caso, en el apartado 2 de dicho artículo, inmediatamente después de definir que se considera «sistema de IA» para el Reglamento, el «riesgo» se erige en otro pilar fundamental de este marco regulatorio, y lo define como: «la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio». No obstante, el marco regulador delimita los sistemas de IA atendiendo al riesgo para la salud, la seguridad o los derechos fundamentales, por lo que no resulta extraña su imprecisa ubicación en el artículo 3 del RIA.

Gracias al trabajo del grupo de expertos de la OCDE. AI⁴¹ sobre incidentes de IA (publicado en mayo de 2024), se han puesto de relieve los muchos daños reales que la IAGen produce y los potenciales daños que puede llegar a producir. Asimismo, queda advertido que el *Monitor de Incidentes de IA de la OCDE* (“AIM”) está lleno de artículos de noticias de varios medios de terceros (en cuanto a la relativa fiabilidad), pero sirve de punto de partida para comprender los desafíos relacionados con la IA. Advierte también la OCDE que esta información de terceros, proporcionada en el AIM, puede contener errores y omisiones, e incluso, pueden estar sujetos a marcas u otros derechos de autor o afines.

⁴⁰ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), de 28 de septiembre de 2022 <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>

⁴¹ La OCDE presentó en mayo de 2024 *Monitor de incidentes de IA de la OCDE* sobre la importancia de la Metodología y divulgaciones de daños reales y probables del desarrollo y uso de la IA, no sin antes advertir que este *paper* se elabora tras monitorear noticias mundiales y que estos perjuicios, muy probablemente, sólo representen un subconjunto de todos los incidentes y peligros de IA en el mundo. <https://oecd.ai/en/incidents-methodology>

Con todo, sirve para vía supuestos acercarnos a una identificación de daños reales y posibles que clarifica los riesgos de los sistemas y modelos de IA de uso general. Así, unos son los perjuicios causados, y otros son potencialmente posibles, por lo es acertado deslindar daños reales de probables en los siguientes términos:

- (i) cuando el evento en el que el desarrollo o uso de un sistema o modelo de IA produce un daño real, se trata de un «incidente de IA»;
- (ii) cuando un evento en el desarrollo o uso de un sistema o modelo es potencialmente perjudicial, se utiliza la expresión «peligro de IA».

¿Cuáles son los daños reales producidos por el mal desarrollo, uso o indebido funcionamiento de la IA? Según lo constatado en este informe de la OCDE, se clasifican en:

- a) lesión o daño a la salud de una persona o grupos de personas;
- b) interrupción de la gestión y operación de infraestructura crítica;
- c) violaciones de derechos humanos o incumplimiento de obligaciones derivadas de la legislación aplicable destinadas a proteger los derechos fundamentales, laborales y de propiedad intelectual;
- d) daño a la propiedad, las comunidades o el medio ambiente.

¿Y los daños potenciales? Un perjuicio probable que puede producirse por el mal desarrollo, uso o indebido funcionamiento de la IA en iguales contextos que los antedichos en la clasificación anterior.

No falta la previsión sobre la debida transparencia a la que alude el artículo 50 del RIA. En este caso, la OCDE advierte de la importancia de divulgar todos estos riesgos y proporcionar una mayor transparencia en el desarrollo de la IA.

3.2. ¿A QUÉ SUJETOS SE DIRIGEN LAS OBLIGACIONES DE EVITAR EL RIESGO? ¿A QUÉ HERRAMIENTAS?

Mientras que el Reglamento, en términos generales, contiene las principales obligaciones a las que está sujeto cualquier operador que participa en la cadena de valor de la IA en el mercado de la Unión, lo que incluye, según el artículo 3, apartado 8, a cualquiera de los siguientes sujetos: *proveedor, fabricante del producto, responsable del despliegue*⁴², *representante autorizado, importador o dis-*

⁴² El denominado «responsable del despliegue» ha sido incorporando en el texto definitivo del Reglamento para referirse en términos generales a quienes utilizan los sistemas de inteligencia

tribuidor, en los modelos de IA de uso general estas obligaciones se limitan al «proveedor», que en el artículo 3, apartado 3) define como: *persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente*⁴³ (fabricantes o desarrollares).

Con estos mimbres, y los precisados en el apartado anterior, conviene señalar dos aspectos esenciales respecto a los modelos de IA de uso general y el cumplimiento del Derecho para evitar o mitigar riesgos para las personas: por un lado, en esta concreta herramienta las obligaciones se dirigen a los proveedores, y si estos incumplen los deberes que le impone el Reglamento -también frente a un proveedor posterior para que lo integre en un sistema de IA-, estamos ante una responsabilidad contractual y el proveedor responderá frente a los organismos de control y frente a proveedores posteriores; por otro lado, si el modelo de IA de uso general falla en su información de salida (*output*) -por error u omisión-, y esto causa daños a terceros, la responsabilidad extracontractual nos proporciona normas propias que según la propuesta de Directiva sobre responsabilidad en materia de IA⁴⁴, difieren de la cobertura que corresponda a un supuesto que, sin ser de alto riesgo, puede ocasionar daños de hondo calado. Su previsión, en la propuesta de Directiva, no está debidamente prevista, y las condiciones acumulativas serán difíciles de probar, a pesar de los riesgos que suponen los modelos.

Si el enfoque uniforme y coherente para los sistemas y modelos de IA proporcionado por el Reglamento está basado en el riesgo de la herramienta, y en función de este se establecen normas comunes y esfuerzos -proporcionales al riesgo- para quienes acometan el desarrollo, la implementación o el uso de esta tecnología, no se entiende que la normativa que se pretende por la Unión para exigir la responsabilidad civil por daños causados a terceros por

artificial bajo su propia autoridad (en la propuesta de la Comisión, de abril de 2021 se utilizó el término «usuario», lo que dio lugar a bastante confusión, y en las enmiendas del Parlamento, de junio de 2023, se adoptó la denominación de «implementador»). El termino finalmente adoptado es mucho más preciso y evita toda suerte de elucubración. Así, según el artículo 3, apartado 4 del RIA, es «responsable del despliegue»: *una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional*.

⁴³ Así se expresa el artículo 3, apartado 3) del RIA, y tras esta definiciones el resto de los sujetos obligados por desarrollar, importar o utilizar sistemas o modelos de IA.

⁴⁴ Los artículo 3 y 4 de la propuesta de Directiva sobre responsabilidad en materia de IA no lo ponen nada fácil para el perjudicado, y ello a pesar de la presunción de la causalidad o del derecho de acceso a las pruebas, una vez que la exigencia de culpa es una cuestión de difícil justificación. El artículo 4, apartado 1, aplicable a todos los sistemas de IA, excepto los de alto riesgo que dificulta la prueba de la culpa y el nexo causal <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>

la IA, se aleje de una responsabilidad objetiva. Este último enfoque, que obligaría a responder al concurrir los elementos esenciales de la responsabilidad civil (acción u omisión, daño y relación de causalidad⁴⁵), se justificaría por el desarrollo mismo de una actividad arriesgada y haría de la IA una herramienta más fiable; propiciaría una respuesta más justa al perjudicado, y además, cumpliría una función disuasoria respecto a los operadores de la IA.

No olvidemos que, por lo pronto, muchos de los sistemas de sistemas «riesgo limitado o medio», entre los que se encuentran los sistemas de IA de uso general que están *basados en un modelo de IA de uso general* (artículo 3, apartado 66): (i) interactúan con seres humanos; (ii) se utilizan para detectar emociones o hacer asociaciones a partir de datos biométricos, o (iii) generan o manipulan contenido. Tengamos también en cuenta que los modelos se integran en sistemas de IA, y aunque de suyo lo hagan en los sistemas de uso general (artículo 3, apartado 66)⁴⁶, nada impide que se integren en sistemas de alto riesgo.

De una manera u otra, la alfabetización en IA sigue siendo una vía incuestionable para mitigar riesgos. Y alertar de los riesgos reales y advertir a organizaciones públicas y privadas, también a la ciudadanía, de la importancia de abordar proactivamente los riesgos asociados con los sistemas y modelos de IA y promover una implementación informada y responsable, una necesidad.

Este tratamiento crítico de la propuesta de regulación de la responsabilidad civil en materia de IA, finalmente, se ha puesto de manifiesto el 19 de septiembre de 2024, en sede del Parlamento Europeo⁴⁷, en una evaluación de impacto realizada a la propuesta inicial de Directiva de responsabilidad civil (de 28 de septiembre de 2022). En esta reciente valoración crítica se pone de manifiesto aquello que hemos reiterado hasta la saciedad: la exigencia de culpa probada en la propuesta de Directiva para la responsabilidad por IA, su influencia en el resultado dañoso, y la presunción de causalidad tras probada

⁴⁵ Al igual que ocurre en el momento presente con la Directiva 85/374, en materia de responsabilidad por los daños causados por productos defectuosos. Así es, que en el artículo 1 de la misma se proclama que el productor responde *de los daños causados por los defectos de sus productos*, y conforme al artículo 4, *el perjudicado deberá probar el daño, el defecto y la relación causal entre el defecto y el daño*.

⁴⁶ A modo meramente recordatorio, es «sistema de IA de uso general»: *un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA*, según el citado artículo 3, apartado 66).

⁴⁷ Por la Comisión de Asuntos Jurídicos (JURI) del Parlamento se presentó, a solicitud de la Comisión un informe acerca de la propuesta de la CE en materia de responsabilidad por IA. Esta *Evaluación de impacto complementaria sobre la propuesta de Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial*, emitida responde a la nueva realidad tecnológica, los modelos de IA de uso general y los sistemas de IA de uso general que también son herramientas de alto impacto. [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU\(2024\)762861_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf)

la conducta reprochable o el incumplimiento, son despropósitos regulatorios que dificultan la función reparadora, también la disuasoria, que debe cumplir un sistema de responsabilidad civil en el que el riesgo es un factor determinante⁴⁸. Además, el informe precisa que la propuesta de Directiva debe ampliar su alcance para incluir sistemas de inteligencia artificial de uso general (basada en modelos) y el *software*⁴⁹ por su alto impacto, y propone, un marco regulatorio que equilibre la responsabilidad a medio camino entre el sistema objetivo y el tratamiento basado en la culpa. Finalmente, en recomendaciones, propugna que el tratamiento de la responsabilidad civil se realice mediante un enfoque uniforme, y en eso, hemos de advertir, una Directiva de mínimos no es la opción adecuada⁵⁰.

4. REFLEXIONES FINALES

En aras de lograr la máxima eficiencia del Reglamento, potenciando la innovación y la protección de los derechos fundamentales de las personas, el marco regulatorio establece normas armonizadas para la IA, y se aplican en todos los sectores, con algunas excepciones (artículos 1 y 2 del RIA). En consonancia con este marco legislativo, se fija que, dicha regulación debe entenderse sin perjuicio del Derecho vigente de la Unión (en protección de datos, de consumidores o derechos fundamentales), que sigue válido e inalterable.

Por otro lado, la regulación de los sistemas de inteligencia artificial presenta un enfoque basado en el riesgo e impone mayor número de obligaciones y requisitos técnicos conforme mayores sean los riesgos del sistema o del modelo. Con todo, también sigue vigente el derecho sustantivo y procesal en cuanto a la tutela de derechos de las personas que puedan verse afectadas o perjudicadas por los modelos y sistemas de IA. Ahora bien, como hemos puesto de manifiesto con anterioridad, el enfoque del riesgo en los sistemas de IA, también en los modelos de IA de uso general, en poco o nada se ha tenido en consideración para propiciar la regulación de la responsabilidad extracontractual por daños causados por la IA. Así es, que mientras en la responsabilidad por producto rige la responsabilidad objetiva, en la responsabilidad por

⁴⁸ Muñoz García, C.) *Regulación de la inteligencia artificial en Europa. Incidencia en los regímenes jurídicos...*, op. cit., p. 184 y ss.

⁴⁹ Al final del Informe sobre el impacto de la Directiva, en la p. 46, se expresa que la propuesta sobre responsabilidad por IA se debería ampliar su alcance para incluir los modelos de IA de propósito general y otros sistemas de IA de alto impacto, también el *software*.

⁵⁰ Así se expresa en el Informe emitido en sede del PE por la Comisión de Asunto Jurídicos, en el apartado 5, p. 38. Y así se puso de relieve en Muñoz García, C. *Regulación...*, cit. ant., p. 184 y pp. 193 y ss.

daños causados por la IA, se parte de una necesaria conducta culposa, que si bien cuenta con presunciones refutables, se aleja de los modelos de responsabilidad objetiva tan coherentes con las actividades arriesgadas.

A la vista de todo lo que está sucediendo en la actualidad, principalmente con la rápida evolución que presentan los modelos de IA de uso general -con GPT a la cabeza-, la gran dependencia de estas herramientas de aprendizaje profundo de los datos de entrenamiento y de la información que circula por la red (en muchas ocasiones de creación humana, publicaciones escritas, audios, música u obras de arte), no hay duda, son innumerables los beneficios pero también los riesgos que estas herramientas conllevan para derechos consolidados en la UE.

Por lo que, además de requisitos y obligaciones por parte de los operadores, y de la máxima transparencia -en su sentido más amplio- desde el diseño, en el desarrollo y uso para generar confianza en los usuarios, es preciso promover la alfabetización en IA y el conocimiento del marco jurídico a todos los individuos, para hacer un uso fiable y eficiente y evitar o minimizar los riesgos que los sistemas de IA conllevan.

Y además, es preciso impulsar una normativa que propicie una protección adecuada a los riesgos que los modelos y sistemas de IA produzcan. Si los riesgos son mayores, los derechos inalterables de los usuarios o terceros no pueden verse desprotegidos. Dicho esto, no es oportuno ofrecer un régimen de responsabilidad basado en la culpa probada, y menos aún, mediante una Directiva de mínimos (responsabilidad civil en materia de IA), que producirá clara fragmentación regulatoria en los EE.MM⁵¹. El criterio del riesgo debería haber sido impulsor para encuadrar la responsabilidad de la IA, también de los modelos de GPAI y el *software* en un modelo de responsabilidad objetiva (cómo lo es en la energía nuclear, o en la navegación aéreas).

De *facto*, el *Monitor de incidentes de IA de la OCDE*, de mayo de 2024, sobre la importancia de la Metodología y divulgaciones de daños reales y probables del desarrollo y uso de la IA es un buen punto de partida para alertar de los riesgos reales y advertir a organizaciones públicas y privadas, también a la ciudadanía, de la importancia de abordar proactivamente los riesgos asociados con los sistemas de IA y promover una implementación informada y responsable. La transparencia y la rendición de cuentas serán esenciales en el desarrollo y uso de una IA segura y confiable

⁵¹ Puesto de manifiesto por Muñoz García, C., op. cit. ant., p. 184.

5. BIBLIOGRAFÍA

- Barrio Andrés, M. (2022). *Manual de Derecho digital*. Editorial Tirant lo Blanch, Valencia, 2.^a edición.
- Barrio Andrés, M. (dir.) (2023). *Legal Tech. La transformación digital de la abogacía*. La Ley, Madrid, 2.^a edición.
- Cotino Hueso, L. y, Castellanos Claramunt J. (dir.) (2022). *Transparencia y explicabilidad de la inteligencia artificial*. Editorial Tirant lo Blanch, Valencia.
- Dignum, V. (2022). *Responsible Artificial Intelligence – from Principles to Practice*. Arxiv, (22 mayo 2022). Visto en <https://arxiv.org/abs/2205.10785v1>
- Dignum, V. (2023) «How Europe is shaping AI for human rights» en *AI Policy Lab*, (5.09.2024). Visto en <https://aipolicylab.se/2024/09/05/how-europe-is-shaping-ai-for-human-rights/>
- Katherine Lee, A. Feder Cooper, James Grimmelmann. (2023). «Talkin’ ‘Bout AI Generation: Copyright and the Generative-AI Supply Chain», *Arxiv*, (15 septiembre 2023). Visto en <https://arxiv.org/abs/2309.08133>
- Muñoz García, C. (2022). 32. «Adaptar o reformular la Directiva 85/374 sobre responsabilidad por daños causados por productos defectuosos a la Inteligencia Artificial». *Diario La Ley. Ciberderecho*, 28 de febrero de 2022. Reeditado como «Adaptar... Últimas novedades y un cambio de rumbo». *Revista Crítica de Derecho Inmobiliario*, vol. 793, noviembre-diciembre 2022, pp. 2886-2908.
- Muñoz GARCÍA, C. (2023). «¿ChatGPT en la universidad? ¿Complementar el aprendizaje y cambiar el modelo educativo?». *Diario La Ley*, núm. 10283, marzo.
- Muñoz GARCÍA, C. (2023). *Regulación de la inteligencia artificial en Europa. Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*. Editorial Tirant lo Blanch, Valencia, 1.^a edición.
- Muñoz García, C. (2024) «Artículo 51 del Reglamento de Inteligencia Artificial», «Artículo 52 del Reglamento de Inteligencia Artificial», «Artículo 53 del Reglamento de Inteligencia Artificial», «Artículo 54 del Reglamento de Inteligencia Artificial», «Artículo 55 del Reglamento de Inteligencia Artificial» y «Artículo 56 del Reglamento de Inteligencia Artificial», todos en *Comentarios al Reglamento de Inteligencia Artificial*, BARRIO ANDRÉS, M, (coord.). Editorial La Ley, Madrid (en prensa).
- Navas Navarro, S. (2023). *ChatGPT y modelos fundacionales*. Editorial Reus, Madrid, 1.^a edición.
- Turin, A.M. (1950). *Computing Machinery and Intelligence*. *Mind* 49: 433-460. Visto en <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>

Responsabilidad por conductas discriminatorias derivadas de los sesgos en el uso de la inteligencia artificial: jurisprudencia y reglamento europeo

ALBERTO MUÑOZ VILLARREAL

Socio de Muñoz Arribas Abogados, S.L.P.

Sumario: 1. INTRODUCCIÓN. 2. ANÁLISIS JURISPRUDENCIAL. 3. EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL. BIBLIOGRAFÍA

1. INTRODUCCIÓN

El gradual desarrollo normativo, jurisprudencial y doctrinal, así como el creciente impacto mediático de los sistemas de Inteligencia Artificial (en adelante IA), muestran la importancia que la misma adquiere en la actual sociedad de la información¹. Y si bien la misma trae aparejados valorables beneficios, sus efectos pueden ser igualmente perjudiciales en diversos ámbitos².

¹ Mi agradecimiento a Iratxe de Anda Rodríguez por su ayuda en la búsqueda de jurisprudencia y a todo el equipo de la Comisión Legal Risk Lab de la Asociación Española de Gerencia de Riesgos y Seguros por sus valiosas aportaciones en las reuniones llevadas a cabo para analizar el riesgo de los sesgos en el uso de Inteligencia Artificial.

² Véase por ejemplo AGUIRRE SALA, JORGE FRANCISCO, “Especificando la responsabilidad algorítmica”, *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, Vol. 19, N.º. 2, 2022 (Ejemplar dedicado a: La educación digital en tiempo del COVID-19).

CÁMARA OUTES, AMANDA, *Responsabilidad civil de productos defectuosos de inteligencia Artificial*, 2023, ICEA-Universidad Pontificia de Salamanca.

TAPIA HERMIDA, ALBERTO, *Sesgos y responsabilidades derivadas de la aplicación de la inteligencia artificial: el caso ChatGPT*, <https://ajtapia.com/2023/04/sesgos-y-responsabilidades-derivadas-de-la-aplicacion-de-la-inteligencia-artificial-el-caso-chatgpt/>

El campo de los Recursos Humanos³ se configura como uno de ellos, debido al considerable impacto que tiene sobre las personas, así como el de Protección de Datos. Entre los desafíos que plantea la IA se encuentra la posibilidad de que se produzcan sesgos en la adopción de decisiones⁴, lo que puede contribuir a la discriminación, incluso por motivos de género o raza.

Ante estas situaciones, la configuración de sistemas de IA se vuelve clave, tanto en el proceso de aprendizaje del algoritmo, como en la elección de las variables a aplicar, o en la calidad de los datos empleados.

La necesidad de confrontar este impacto, a veces incluso indirectamente discriminatorio (sea por asociación, por discriminación múltiple o por error), requiere de algoritmos que empleen normas de derecho antidiscriminatorio, que sean transparentes y que funcionen en aras de la equidad, la rendición de cuentas e inclusive que promuevan la diversidad cultural. Así, ante la dificultad de percibir aquellas configuraciones discriminatorias, la legislación más reciente opta por realizar una clasificación de los sistemas de IA en función de su riesgo, así como la posibilidad de que, en supuestos concretos, los proveedores de sistemas sean capaces de tratar categorías especiales de datos a fin de mitigar posibles amenazas.

2. ANÁLISIS JURISPRUDENCIAL

La existencia de sesgos algorítmicos en el diseño de sistemas de IA⁵ empleados en gestión de Recursos Humanos ha dado lugar, en distintos países

³ La optimización de los procesos de Recursos Humanos mediante Inteligencia Artificial es un tema de actualidad en cuanto puede suponer en una mejora sustancial en su eficiencia al automatizar parte de ellos y generar conocimiento adicional que a su vez mejora la productividad en los procesos de negocio. Cuanto más intensivo en el factor trabajo sea un sector determinado, mayor será la utilidad marginal potencial del uso de la IA.

⁴ “Totalmente ligado al respeto a la autonomía se encuentra el principio de explicabilidad o de trazabilidad, según el cual, los afectados tenemos derecho a controlar el uso de nuestros datos y a conocer los algoritmos que los manejan. Porque los seres humanos tienen sesgos, como se ha mostrado hasta la saciedad, pero también los sistemas autómatas los tienen y son más invisibles que en el caso de los humanos. Entre otras razones, porque los diseñadores introducen los sesgos en los sistemas inteligentes, consciente o inconscientemente”, CORTINA ORTOS, ADELA, “Ética de la inteligencia artificial”, *Anales de la Real academia de Ciencias Morales y Políticas* N. 96, 2019, pág. 390.

⁵ Entendemos por sistemas de Inteligencia Artificial aquellos “que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía con el fin de alcanzar objetivos específicos”. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia Artificial para Europa. 26 de junio de 2018. COM (2018) 237.

de nuestro entorno, a pronunciamientos judiciales que concluyen que se han producido situaciones discriminatorias prohibidas por la normativa.

Por ejemplo, en Italia la Sentencia del Tribunal Ordinario de Bolonia 2949/2020, de 31 de diciembre N.R.G. 2949/2019⁶, que analiza un caso en que un algoritmo contaba con dos parámetros a la hora de valorar a los trabajadores, siendo estos la fiabilidad y disponibilidad. Sin embargo, a la hora de cumplir con dichos parámetros no tuvieron en cuenta circunstancias del trabajador como el derecho a huelga, baja por enfermedad o accidentes de trabajo, de tal modo que se produciría una discriminación hacia determinados trabajadores al no valorar los derechos, produciéndose por tanto una discriminación indirecta⁷.

En síntesis, el algoritmo empleado por Deliveroo Italia S.R.L., puntuaba negativamente tanto la falta de puntualidad como una situación de incapacidad temporal, sin tener en cuenta las circunstancias particulares de cada situación con lo que conculcaba el principio de no discriminación e igualdad de trato.

Mientras que la Sentencia del Consejo de Estado, Sección Sexta, de 8 de abril de 2019, N. 02270/2019REG.PROV.COLL. N. 04477/2017 REG.RIC⁸ abordó un caso en que unos profesores candidatos a ser contratados denunciaron que todo el procedimiento de selección había sido gestionado por un sistema informático que utilizaba un algoritmo cuyo funcionamiento se desconocía. Este no solo había dado lugar a medidas sin justificación alguna, sino que tampoco se había identificado al funcionario de la administración que había evaluado las situaciones individuales y expresado correctamente las decisiones provisionales pertinentes. Según los recurrentes, este algoritmo habría dispuesto traslados a una provincia y no a otra, a una posición de apoyo y no a una posición común, sin tener en cuenta las preferencias indicadas en las respectivas solicitudes de transferencia, sin motivación alguna y en defecto de la más mínima transparencia.

La Sentencia considera que

“se violan los principios de imparcialidad, publicidad y transparencia, al no quedar claro por qué las expectativas legítimas de sujetos ubicados en una posición específica en la clasificación se sintieron decepcionados.

⁶ Disponible para su consulta en Ordinanza_Bologna.pdf (laboral-social.com).

⁷ Véase FERNÁNDEZ SÁNCHEZ, Sonia, “Frank, el algoritmo consciente de Deliveroo. Comentario a la Sentencia del Tribunal de Bolonia 2949/2020, de 31 de diciembre”, *Revista de Trabajo y Seguridad Social*. CEF, 457 (abril 2021), pp. 179-193.

⁸ Disponible en:

https://portali.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=201704477&nomeFile=201902270_11.html&subDir=Provvedimenti

De hecho, la imposibilidad de comprender los métodos con los que, a través del citado algoritmo, se asignaron las plazas disponibles, constituye en sí misma una falla capaz de invalidar el procedimiento.

No sólo eso, los resultados de las mismas parecen caracterizarse por la falta de lógica e irracionalidad denunciadas por los recurrentes, habiéndose producido situaciones paradójicas en las que docentes con varios años de servicio fueron asignados a áreas territoriales nunca solicitadas y ubicadas a cientos de kilómetros de las suyas, mientras que otros docentes, con menor titulación y menor antigüedad, obtuvieron las mismas plazas que solicitaron”⁹.

En Reino Unido la Sentencia del Tribunal de Empleo 3206212/2021, del East London Hearing Centre de 19 de mayo de 2022¹⁰, abordó el caso *Manjang versus Uber Eats*¹¹. Este caso en concreto derivaba de la terminación de un contrato por discriminación laboral indirecta en el cese de un conductor de Uber en Reino Unido, toda vez que la empresa introdujo un sistema de reconocimiento facial con sesgo étnico. El trabajador de origen africano había estado trabajando en la empresa desde 2019, pero la introducción de este nuevo modelo de registro de jornada dio lugar a continuos fallos por falta de verificación por la aplicación electrónica. El demandante nunca había sido informado sobre los procesos que llevaron a su suspensión, ni los parámetros del sistema de IA encargado del reconocimiento.

Otra resolución, si bien no se trata de una Sentencia, de poderosa relevancia se encuentra en la decisión adoptada por la Autoridad de Países Bajos de los Países Bajos (‘DPA’). Sentando importante precedente para futuros casos, enjuicia las actividades llevadas a cabo por la mercantil estadounidense Clearview, cuya actividad se basaba en ofrecer servicios de reconocimiento facial para actividades de inteligencia e investigación. A modo de ejemplo, Clearview realizaba reconocimientos faciales a partir de las imágenes grabadas por cámaras, contrastándolas con su propio registro de más de 30 billones de fotografías obtenidas de internet. Además, hay que decir que no se había obtenido consentimiento de aquellos usuarios cuyas fotografías se trataban.

Analizado el caso, la DPA resolvió que Clearview (i) trataba datos personales sin base jurídica, infringiendo el artículo 5.1.a) RGPD en relación al artículo 6.1 RGPD; (ii) trataba una categoría especial de datos personales (biométricos) infringiendo el artículo 9.1 RGPD; (iii) no informaba a los interesados del tratamiento *ex art.* 12 RDPD en relación con el artículo 14.1 y 14.2 RGPD;

⁹ Hecho 9 de la Sentencia, la traducción es nuestra.

¹⁰ Disponible para su consulta en *Mr P E Manjang v Uber Eats UK Ltd and others*: 3206212/2021 - GOV.UK (www.gov.uk)

¹¹ *Mr P E Manjang v Uber Eats UK Ltd and others*: 3206212/2021, disponible en <https://www.gov.uk/employment-tribunal-decisions/mr-p-e-manjang-v-uber-eats-uk-ltd-and-others-3206212-slash-2021>.

(iv) y negó en distintas ocasiones las solicitudes presentadas por estos últimos de acceso a sus datos personales, violando lo dispuesto en los artículos 12.2 y 15 RGPD, al imposibilitar el derecho de acceso a sus datos.

Pero lo que demuestra esta resolución va mucho más allá. Si bien la compañía estadounidense fue condenada con multas que ascendían a varios millones de euros, las autoridades neerlandesas también decidieron imponer hasta cuatro órdenes sujetas a sanción por incumplimiento de la normativa de protección de datos, así como por no poner fin a las infracciones enjuiciadas.

En este sentido, Clearview no opera a través de un establecimiento en Europa. Esto tiene su reflejo en que las autoridades del país ya habían puesto de manifiesto que Clearview vulneraba la normativa de protección de datos, pero la compañía no ponía fin a dichas infracciones. Desde entonces, los distintos organismos competentes buscan formas de asegurar el fin de su conducta, por ejemplo, investigando si los directivos de la empresa pueden ser considerados personalmente responsables de las infracciones¹².

En España podemos destacar la Sentencia de la Audiencia Nacional (Sala de lo Social) 104/2021, de 10 de mayo [AS 2021/1257, ECLI: ECLI:ES:AN:2021:1855] relativa al empleo de un algoritmo de control programático de las pausas permitidas al trabajador durante su jornada de teletrabajo. La empresa requería que todos los trabajadores estuviesen continuamente conectados, ante lo cual el Tribunal falla que se trata de una práctica discriminatoria por cuanto no otorga igualdad de condiciones a aquellas personas que, por razón de edad, cuentan con unas necesidades fisiológicas más apremiantes.

Así en el Fundamento Jurídico 4 se indica que:

“(…) es claro que debe accederse a la pretensión de CCOO por cuanto que el sistema de registro de jornada que tiene implementado la empresa en todas sus plataformas excepto en la de Málaga implica en la práctica que los trabajadores únicamente pueden realizar sus necesidades fisiológicas en aquellos momentos en los que la empresa, bien ha programado pausa por PVD o bien en coincidiendo con la tradicionalmente denominada como “pausa del bocadillo”, en esta litis referenciada como “pausa de comida”, de forma que si han de interrumpir su actividad para acudir a satisfacer tal necesidad inevitable se ven obligados a registrar un descanso en un momento no programado por la empresa, bien a no registrarlo y desatender su puesto de trabajo, pudiendo ser sancionados por tales motivos.

Pues bien, en el presente caso- en el que como hemos dicho el trabajador está en todo momento conectado telefónica y digitalmente-, el no permitir registrar pausas vul-

¹² Sentencia y nota de prensa disponible en: Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition | Autoriteit Persoonsgegevens

nera la dignidad del trabajador, que no es otra cosa que el derecho que tiene a ser tratado como una persona en todo momento, resulta contrario a la protección de salud, y, aun cuando no se haya alegado esta Sala a mayor abundamiento y “obiter dictae” considera que puede constituir una discriminación indirecta por razón de edad proscrita por el art. 17.1 del E.T pues resulta indiscutible que esta práctica, aparentemente neutra, implica en la práctica un trato peyorativo a los trabajadores de más edad respecto de los más jóvenes”.

Además del ámbito del derecho laboral, numerosos tribunales se han pronunciado sobre la vulneración de datos personales por el empleo de sistema de Inteligencia Artificial. Ejemplo de ello es la Sentencia del Tribunal de Justicia del Tribunal de Justicia de la Unión Europea de 7 diciembre 2023, OQ contra Land Hessen, C-634/21 (ECLI:EU:C:2023:957)¹³. La sentencia tiene como trasfondo el algoritmo de la empresa SCHUFA, agencia de información sobre solvencia de terceros. El algoritmo tenía como fin la generación automatizada de valores de puntuación crediticia (o *credit scoring*). A través de una serie de procedimientos matemáticos y estadísticos, y un análisis del historial de solvencia de diferentes consumidores, el algoritmo permitía predecir la posibilidad de que un determinado cliente falte al pago de sus deudas. El demandante había visto su crédito denegado en base a la ejecución de dicho algoritmo y el tribunal alemán, donde la *litis* tenía su origen, plantea una cuestión prejudicial sobre si, pese a que no es la entidad bancaria la que emite la decisión automatizada, -sino la agencia de información que únicamente genera valor de probabilidad-, esto puede entrar dentro de la definición de decisión individual automatizada.

El Tribunal Europeo procede a hacer una interpretación garantista de la finalidad del artículo 22 del Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y de la normativa de protección de datos en su conjunto (en adelante RGPD).

El citado artículo, relativo a las decisiones individualizadas automatizadas, incluida la elaboración de perfiles, estipula que

“1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

¹³ Disponible en <https://op.europa.eu/es/publication-detail/-/publication/acd82fb9-94e3-11ee-b164-01aa75ed71a1/language-es>

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado”.

El Alto Tribunal Europeo, analizado el artículo 22 y el algoritmo que dio origen a la causa, entiende que, en este caso, un consumidor, como resultado de la valoración insatisfactoria del algoritmo, verá su concesión de préstamo denegada. En este sentido, dado que el valor de probabilidad influye de manera determinante en la decisión de un tercero, y aunque una primera lectura del artículo 22 RGPD pueda dar a entender que se dirige únicamente a la empresa que es la emisora de la decisión final, la realidad es otra.

Así, una “decisión individual automatizada” ha de aplicar igualmente en aquellos supuestos en los que influye de manera esencial en la valoración realizada por el emisor de la decisión. El Tribunal Europeo entiende que existe una laguna en la protección jurídica si se optará por una interpretación restrictiva y opta por concepto amplio de la “decisión”.

El ámbito de aplicación del artículo 22 RGPD y, las restricciones sobre las decisiones automatizadas, no se restringen únicamente a unas decisiones totalmente automatizadas, sino también cuando puede tener un efecto similar. No obstante, la protección que despliega en otras naciones europeas no tiene siempre y en todo caso la misma intensidad.

En Holanda resultas relevantes los casos Uber y Ola, ambas compañías de vehículos de transporte con conductor, y cuyos procedimientos se sustanciaron ante el Tribunal de Distrito de Ámsterdam (Sentencias del Tribunal de Distrito de Ámsterdam Asunto C/13/687315 / HA RK 20-207 de 11 de marzo de 2021, ECLI:NL:RBAMS:2021:1020¹⁴, y Asunto C/13/689705 / HA

¹⁴ Disponible en <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1020>

RK 20-258 de 11 de marzo de 2021, ECLI:NL:RBAMS:2021:1019¹⁵. En síntesis, si bien la causa comenzó por una solicitud de datos a sendas compañías en base al artículo 15 RGPD para probar las notas de laboralidad que mantenían con los conductores, el procedimiento requirió de la aplicación del artículo 22 RGPD. El grado de automatización de los controles realizados por los algoritmos de las empresas eran esenciales a la hora de probar los indicios de la relación laboral.

Y pese a que el caso Uber se desestimó, en lo que aquí interesa, por falta de motivación suficiente sobre los “efectos jurídicos” que alegaban que producía el algoritmo -o decisión que le afectaba “significativamente de modo similar”-; en el caso Ola el tribunal realizó un análisis más extenso de los algoritmos empleados -perfil de conductor, sistema de detección de irregularidades, sistema de asignación de viajes, etc.-. No obstante, el Tribunal de Distrito entendió que, si bien dichos parámetros podían tener efecto en el comportamiento de los conductores, los mismos no habían probado que los resultados consistían en efectos jurídicos o afectación similar del artículo 22 RGPD. Todo ello excepto para los supuestos de “sanciones y deducciones” (párrafo 4.51). Aquí, el tribunal consideró que las sanciones y deducciones sí tenían efectos similares capaces de perjudicarles significativamente, por lo que procedía requerir a la empresa para que compartiese la lógica del algoritmo *ex art.* 15 RGPD.

Sin perjuicio de lo anterior, la apelación de las anteriores sentencias del Tribunal de Distrito, aumentaron considerablemente el ámbito de aplicación del artículo 22 y 15 RGPD. La Sentencia del Tribunal de Apelación de Ámsterdam, Departamento de Derecho civil y Tributario, Equipo I, Asunto 200.295.742/01 de 4 de abril de 2023, ECLI:NL:GHAMS:2023:793¹⁶ concluyó que Uber sí debía proporcionar información relacionada con la toma de decisiones automatizada, ya que los conductores estaban significativamente afectados por las decisiones y la compañía no logró probar como se produce la intervención humana.

Además, que el artículo 15 RGPD no permitía eximirse basándose en la protección de secretos comerciales, tratándose de un argumento desproporcionado *vis-à-vis* los efectos que tenían las decisiones automatizadas sobre los conductores. Por ello, se requirió a la multinacional para proporcionar la información sobre los factores y ponderaciones en las decisiones de viaje, tarifas o calificaciones.

La apelación de Ola también dio lugar a consecuencias similares. La Sentencia del Tribunal de Apelación de Ámsterdam, Departamento de

¹⁵ Disponible en <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1019>.

¹⁶ Disponible en: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793>.

Derecho civil y Tributario, Equipo I, Asunto 200.295.806/01 de 44 de abril de 2023, ECLI:NL:GHAMS:2023:804¹⁷ condena a la empresa a facilitar información sobre las valoraciones de los conductores, siempre y cuando no se permita identificar a los usuarios que remitieron dichas calificaciones. Además, también debía facilitar información sobre la toma de decisiones automatizadas respecto, entre otros, a las puntuaciones de probabilidad de fraude de los conductores; perfiles de ingreso; o el sistema de tarifas.

El caso de la aplicación SyRI¹⁸, fue enjuiciado en la Sentencia del Tribunal de Distrito de La Haya, C / 09/550982 / HA ZA 18-388, de 5 de febrero de 2020. El Sistema de Indicadores de Riesgo es un instrumento desarrollado por el gobierno neerlandés con el objetivo de prevenir y combatir el fraude a la Seguridad Social, que realiza un informe de riesgos sobre las probabilidades de defraudar al sistema de la Seguridad Social a través de grandes cantidades de datos obtenidos por diversas administraciones públicas que colaboran en el intercambio de datos con la plataforma.

Uno de los principales problemas por lo que este algoritmo fue a la Corte de Distrito de la Haya era por si la aplicación SyRI infringía o no el derecho a la privacidad. Según los arts. 93 y 94 de la Constitución neerlandesa, la Corte entiende que ante esta normativa debe aplicarse el derecho humano al respeto a la vida privada y familiar del art. 8 de la Carta Europea de Derechos Humanos a partir de la interpretación que del mismo ha hecho el Tribunal Europeo de Derechos Humanos y, en este sentido, determina que este derecho está íntimamente relacionado con el derecho a la protección de los datos personales. Del mismo modo, se examina la Carta de los Derechos Fundamentales (arts. 7 y 8) y el RGPD.

A partir de estas precisiones, se valora el derecho a la privacidad, llegando a la conclusión de que no se puede evaluar con exactitud qué es este algoritmo ni como es su mecanismo, dado que el Gobierno no ha hecho pública - ni ha aportado al procedimiento - información objetiva y verificable sobre el modelo de riesgo en el que se basa. Además, la normativa neerlandesa no prevé ninguna obligación de informar a aquellas personas cuyos datos son procesados o incluso de que se les esté aplicando un informe de riesgo. De esta manera, aunque en este caso no parecía existir ningún sesgo o discriminación, este algoritmo digital si que presentaba problemas en relación a la privacidad, resultando ser la normativa insuficiente, así como el propio algo-

¹⁷ Disponible en: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:804>.

¹⁸ LAZCOZ MORATINOS, GUILLERMO y CASTILLO PARRILLA, JOSÉ ANTONIO "Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI, Revista *Chilena de Derecho y Tecnología*, 2020, n. 1, p. 208.

ritmo, en lo que respecta a su injerencia desproporcional en la vida privada de las personas.

El uso de herramientas de inteligencia artificial generativas en procesos judiciales fue objeto de la Sentencia de la Sala Segunda de Revisión de la Corte Constitucional de Colombia, dictada el 2 de agosto de 2024, T-323¹⁹. En ella se abordaron los siguientes puntos (i) el derecho fundamental al debido proceso; (ii) el debido proceso en un sistema jurisdiccional que utiliza IA; (iii) el sistema de inteligencia artificial. Conceptos y aspectos básicos acerca de su funcionamiento; (iv) impactos del uso de herramientas de IA en la sociedad; (v) estado de la IA en Colombia; (vi) el marco regulatorio de la IA en el mundo. Algunos instrumentos de *soft law* e iniciativas normativas nacionales; (vii) algunas experiencias concretas relacionadas con la IA en la práctica judicial; (viii) la garantía del juez natural en un sistema jurisdiccional que utiliza IA y (ix) el debido proceso probatorio en un sistema jurisdiccional que utiliza IA.

En cuanto a la posible violación al debido proceso por la sentencia de segunda instancia, al utilizar el juez ChatGPT para su motivación, la Sala estimó que no existió un remplazo del ejercicio de la función jurisdiccional por parte de ChatGPT, esencialmente porque el sistema de IA se utilizó luego de haberse fundamentado y tomado la decisión.

En el orden metodológico que adoptó el fallo de tutela, el funcionario judicial primero identificó la tesis que sostendría, luego las normas constitucionales aplicables al caso, el referente jurisprudencial que se debía atender por guardar identidad fáctica con el asunto analizado, para, posteriormente, solucionar el caso concreto al indicar que el cobro de copagos y cuotas moderadoras constituía una barrera de acceso al servicio de salud del niño. Solo entonces, anunció y procedió a efectuar preguntas en el referido sistema de IA, para así transcribir las respuestas arrojadas en la consulta.

Conforme con lo anterior, no se cuestionó la validez de la decisión del Juzgado del Circuito por haber sido tomada con antelación al uso de la herramienta ChatGPT. Sin perjuicio de lo anterior, se evidenció que no se cumplieron a cabalidad los principios de transparencia y responsabilidad exigidos. En cambio, el principio de privacidad sí se satisfizo, pues el juez no introdujo datos personales del menor ni de su historia clínica, ni de las partes involucradas en la disputa concreta. Respecto al asunto de fondo, la Corte estimó que en el presente caso se cumplían las condiciones para exonerar al menor de edad del cobro de copagos y cuotas moderadoras con ocasión de los servicios y medicamentos que requiera, ya que las leyes 1438 de 2011 y 1618 de 2013,

¹⁹ Disponible para su consulta en <https://www.corteconstitucional.gov.co/relatoria/2024/T-323-24.htm>

así como el Decreto 1652 del 2022, exceptuaban del cobro de cuotas moderadoras y copagos a las personas en situación de discapacidad, en relación con su rehabilitación.

La Entidad Promotora de Salud ('EPS'), aunque exoneró al niño de los copagos y cuotas moderadoras, no comunicó ni informó a las Instituciones Prestadoras de Servicios de Salud ('IPS') sobre la gratuidad de los servicios y medicamentos ordenados al niño, lo cual generó una barrera administrativa para la prestación oportuna de los servicios médicos, situación que va en detrimento de los principios de accesibilidad e integralidad del SGSSS.

Por otro lado, la Sala encontró acreditado que (i) ni el niño ni su madre tienen los recursos económicos suficientes para pagar el valor de los traslados requeridos para acceder al servicio de salud, pues se encuentran en situación de pobreza extrema y (ii) la falta de autorización del transporte, debido al diagnóstico que padece el niño, pondría en riesgo su dignidad y estado de salud. Si bien la EPS autorizó el suministro del transporte para la asistencia a las terapias de rehabilitación de su hijo, no se dio orden respecto a los demás desplazamientos asociados a valoraciones y controles con especialistas y ayudas diagnósticas. De acuerdo con ello, la Sala encontró una deficiencia en el amparo concedido por los jueces de instancia, pues la orden impartida no garantiza efectivamente la plena protección de los derechos fundamentales del niño a la salud y la vida digna.

Finalmente, sobre el tratamiento integral no se allegó prueba al expediente de que la EPS se negara a autorizar alguna orden médica que prescribiera una valoración, tratamiento, servicio asistencial, ayuda diagnóstica, control o cualquier otro parecido para la atención médica del niño, por lo que no procede ordenar nada adicional a lo ya planteado anteriormente.

La Sala de Revisión decidió que el derecho al debido proceso no se había vulnerado por el juez de segunda instancia, por tanto, no se configuró una causa de invalidez de lo actuado, pues el uso de ChatGPT en el caso sometido a estudio no comportó una usurpación de la función de administración de justicia a cargo de la autoridad judicial competente.

Sin perjuicio de lo anterior, la Sala estimó que en el marco del respeto a los derechos fundamentales y de la salvaguarda de las garantías constitucionales para los usuarios del sistema de administración de justicia, y dadas las posibilidades de alucinaciones, sesgos discriminatorios y demás riesgos asociados a la IA, era procedente establecer algunos criterios orientadores, así como que, desde el Consejo Superior de la Judicatura, se emitieran unas guías o lineamientos sobre su implementación por parte de los jueces. También que desde la judicatura misma se adoptaran las mejores prácticas que conforme

a los principios y mandatos constitucionales, permitan hacer uso razonable y proporcional de herramientas innovadoras y dinámicas como ChatGPT, sin admitir en modo alguno que se impacte el debido proceso o se restrinjan de cualquier forma la autonomía e independencia judiciales.

En cuanto a los derechos del niño, la Sala confirmó parcialmente la sentencia. Esto, debido a que se encontraron fallas en la completa salvaguarda de los derechos vulnerados. Así, (i) la Sala de Revisión consideró procedente para la garantía efectiva del amparo concedido por los jueces de instancia ordenar a la EPS que realicen todas las gestiones y trámites administrativos necesarios para que las IPS encargadas de la atención del niño aplicaran diligentemente y sin demoras la exoneración de cobros de copagos y cuotas moderadoras, sin trasladar al niño y a su representante las consecuencias negativas de las eventuales faltas de comunicación entre las entidades del sistema; (ii) estimó procedente modificar los términos en que los jueces de instancia ordenaron a la EPS autorizar el servicio de transporte intermunicipal, ya que no se debía limitar dicho reconocimiento al transporte requerido para asistir a las terapias prescritas en la valoración médica del 19 de julio de 2022. La EPS debe suministrar el servicio de transporte las veces que requiera el niño según criterio médico, para el tratamiento de su diagnóstico de trastorno de espectro autista, mientras subsista la insuficiencia de recursos económicos de sus padres para asumirlas; y (iii) la accionante no reprochó ninguna actitud pasiva u omisiva con la que la EPS accionada estuviese negando el tratamiento integral, por lo que es innecesario tomar una medida al respecto.

La Sentencia n° 2020-834 QPC de 3 de abril de 2020 del Consejo Constitucional francés²⁰ analiza la comunicabilidad y publicidad de los algoritmos implementados por las instituciones de educación superior para el examen de las solicitudes de inscripción en el primer ciclo. Concluye que la restricción de acceso a determinados documentos administrativos relativos a los posibles tratamientos algorítmicos utilizados por la institución no quita efectividad a los recursos contra una decisión de denegación de inscripción.

En el ámbito del derecho penal en Estados Unidos contamos con la Sentencia²¹ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), Case number 2015AP157-CR. El juez de instancia utilizó los datos proporcionados por COMPAS, una herramienta de valoración de las posibilidades de reincidencia de los criminales, que indicó que el encausado presentaba un riesgo alto tanto de reincidencia en general como de reincidencia violenta, lo cual tuvo en cuenta a la hora de imponer la pena. El condenado solicitó la revisión de la

²⁰ Disponible en <https://www.conseil-constitutionnel.fr/es/decision/2020/2020834QPC.htm>

²¹ Disponible en [https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap_000157-cr.html#:~:text=The%20Supreme%20Court%20affirmed,%20holding%20\(1\)%20if%20used](https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap_000157-cr.html#:~:text=The%20Supreme%20Court%20affirmed,%20holding%20(1)%20if%20used)

pena, pues la misma al fundarse en el resultado de COMPAS vulneraba su derecho a un proceso debido. Pero el tribunal no modificó la condena, pues el resultado de la herramienta solo lo usó para corroborar las conclusiones a las que ya había llegado a partir del resto de información disponible. El Tribunal Supremo del Estado de Wisconsin no estimó el recurso presentado, pero si es verdad que estableció algunas limitaciones sobre cómo y para qué pueden ser usadas las evaluaciones de riesgo en la fase de determinación de la pena.

3. EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (en adelante Reglamento IA), aborda la cuestión de estudio en varios aportados²².

²² La publicación del RIA no implicará la inmediata aplicabilidad de la norma ya que, según el texto de su artículo 85, si bien el Reglamento entrará en vigor a los 20 días su publicación en el DOUE, solo será aplicable a los 24 meses de su entrada en vigor.

No obstante, sus títulos I (Disposiciones generales) y II (Sistemas de IA prohibidos), se aplicarán a partir de seis meses de su entrada en vigor. El Capítulo 4 (Autoridades notificantes y organismos notificados) del Título III (Sistemas de IA de alto riesgo); el Título VI (Gobernanza), el Título VIII bis (Modelos de IA de propósito general) y el Título X (Sanciones) se aplicarán a partir de doce meses de la entrada en vigor y el apartado 1 del artículo 6 (Normas de clasificación de los sistemas de IA de alto riesgo) y las obligaciones correspondientes del presente Reglamento se aplicarán a los 36 meses de la entrada en vigor.

Pacto sobre IA

Es por ello por lo que la Comisión ha planteado el que denomina “Pacto sobre IA” (AI PAct), buscando el compromiso voluntario de la industria de comenzar a aplicar los requisitos del Reglamento antes de dicho plazo legal.

Una circunstancia que se considera tanto más importante cuanto que en los últimos meses se han acelerado los avances tecnológicos y la adopción generalizada de sistemas de IA generativos y de propósito general.

Mediante su adhesión al Pacto sobre IA, las empresas de la UE y de fuera de la UE tendrán la oportunidad de demostrar y compartir su compromiso con los objetivos de la futura Ley de IA y prepararse desde el principio para estar listos para su implementación, participando además en una comunidad de intercambio de buenas prácticas, orientada a aumentar la sensibilización sobre los principios que sustentan la futura Ley de IA, y (en el momento de su adopción) garantizar el compromiso de anticipar y colmar la brecha antes de la aplicabilidad del Reglamento sobre IA.

Más específicamente, el Pacto alentará a las empresas a comunicar voluntariamente los procesos y prácticas que están implementando para prepararse para el cumplimiento y garantizar que el diseño, el desarrollo y el uso de la IA sean confiables.

El Reglamento de Inteligencia Artificial aborda los riesgos asociados a usos específicos de la IA, los clasifica en cuatro niveles de riesgo y establece normas diferentes para cada nivel.

Los cuatro niveles de riesgo del Reglamento de IA y sus normas correspondientes son:

- Riesgo mínimo o nulo: la mayoría de los sistemas de IA no plantean riesgos. Los juegos o los filtros de correo no deseado basados en la IA pueden utilizarse libremente, puesto que no están regulados ni se ven afectados por el Reglamento de IA de la UE.
- Riesgo limitado: los sistemas de IA que comportan un riesgo limitado, como los chatbots o los sistemas de IA generadores de contenido, están sujetos a obligaciones de transparencia, como la de informar a los usuarios de que su contenido se ha generado mediante IA para que puedan tomar decisiones con conocimiento de causa sobre su uso posterior.
- Riesgo alto: los sistemas de IA de alto riesgo, como los utilizados en el diagnóstico de enfermedades, la conducción autónoma y la identificación biométrica de personas implicadas en actividades delictivas u objeto de investigaciones penales, deben cumplir unos requisitos y obligaciones estrictos para acceder al mercado de la UE. Entre ellos se incluyen unas pruebas rigurosas, de transparencia y supervisión humana.
- Riesgo inaceptable: está prohibido en la UE el uso de sistemas de IA que supongan una amenaza para la seguridad, los derechos o los medios de subsistencia de las personas. Están prohibidos, por ejemplo,

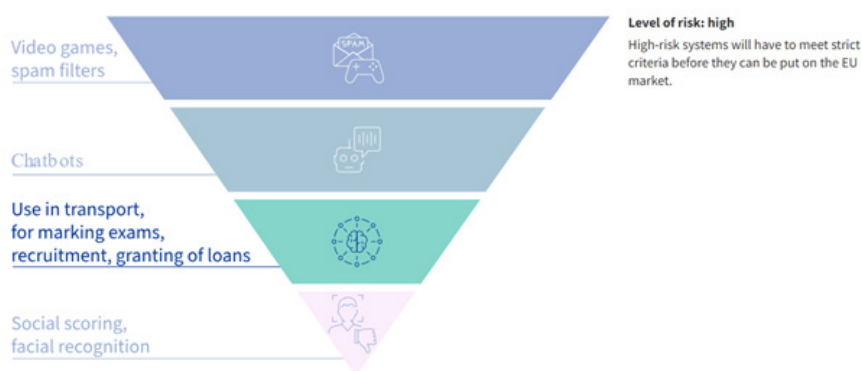
Estos compromisos de la industria adoptarán la forma de compromisos (declaraciones de compromiso, o *declarations of engagement*) y deberán incluir detalles sobre las acciones concretas que se estén llevando a cabo o estén planificadas para abordar los requisitos específicos de la futura Ley de IA. Estos compromisos pueden incluir un enfoque gradual, es decir, esbozar planes para avanzar, dentro de un plazo definido, hacia niveles más altos que las acciones ya implementadas.

Estos compromisos asumidos por las empresas que se adhieran al Pacto serán recogidos y publicados por la Comisión, con el fin de proporcionar visibilidad, aumentar la credibilidad y aumentar la confianza en las tecnologías desarrolladas por las empresas que participan en el Pacto.

La Comisión se compromete a colaborar con los participantes en este Pacto, apoyándolos en:

- La construcción de una comprensión común de los objetivos de la futura Ley de IA;
- La adopción de medidas concretas para comprender, adaptar y preparar la futura aplicación de la Ley de IA (por ejemplo, crear procesos internos, preparar al personal y autoevaluar los sistemas de IA);
- Compartir conocimientos y aumentar la visibilidad y credibilidad de las salvaguardias establecidas para demostrar una IA fiable; y en última instancia
- Generar confianza adicional en las tecnologías de IA.

la manipulación cognitiva conductual, la actuación policial predictiva, el reconocimiento de emociones en lugares de trabajo y centros educativos, y la puntuación ciudadana, así como -con algunas excepciones- el uso en los espacios públicos, por parte de las autoridades garantes del cumplimiento del Derecho, de sistemas de identificación biométrica remota en tiempo real, como el reconocimiento facial.



Fuente: Consejo Europeo:

<https://www.consilium.europa.eu/es/policies/artificial-intelligence/#0>

El Reglamento de IA dedica gran parte de su articulado a regular los sistemas de alto riesgo, que divide en dos grandes subgrupos: Por un lado, mediante un análisis de riesgos se ha identificado un conjunto de familias de sistemas de IA que pueden considerarse de alto riesgo si su salida es relevante respecto a una acción o decisión que pueda presentar un riesgo a la salud, la seguridad, o los derechos fundamentales. Además, enumera y describe este conjunto, que incluye, entre otros, sistemas de identificación biométrica, de protección de infraestructuras críticas, de selección y promoción de personal, de utilización en fronteras, o los usados por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración de Justicia. La Comisión puede actualizar esta lista mediante un acto delegado²³.

El Reglamento busca la aplicación de los principios de no discriminación y equidad, lo que se produce cuando los sistemas de IA se desarrollan y uti-

²³ Por otro lado, existen productos que ya están regulados por normativa armonizada de la UE, y que bajo esa normativa están sujetos a evaluación de conformidad. Hay un conjunto limitado de familias de estos productos, que incluye entre otros los dispositivos médicos, los trenes o la maquinaria. Un sistema IA que constituya uno de estos productos, o constituya un componente de seguridad de uno de estos productos, estará sujeto a su correspondiente normativa armonizada.

lizan de un modo que incluya a diversos agentes y promueva la igualdad de acceso, la igualdad de género y la diversidad cultural, al tiempo que se evitan los efectos discriminatorios y los sesgos injustos prohibidos por el Derecho nacional o de la Unión.

Entre lo sistema de IA de alto riesgo²⁴ se califican los destinados a la administración de justicia pues, a fin de hacer frente al riesgo de posibles sesgos, errores y opacidades, la Unión Europea entiende que procede clasificar como de alto riesgo aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos.

En cuanto a la gobernanza de datos, prevé que los conjuntos de datos deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los colectivos de personas en relación con los que esté previsto utilizar el sistema de IA de alto riesgo, prestando una atención especial a la mitigación de los posibles sesgos en los conjuntos de datos que puedan afectar a la salud y la seguridad de las personas físicas, tener repercusiones negativas en los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando los datos de salida influyan en la información de entrada de futuras operaciones (bucles de retroalimentación).

Los sesgos, por ejemplo, pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generados cuando los sistemas se despliegan en entornos del mundo real. Los resultados de los sistemas de IA dependen de dichos sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente -en particular con respecto a las personas pertenecientes a determinados colectivos vulnerables, incluidos colectivos raciales o étnicos-.

²⁴ “El RIA sitúa, por ello, su centro de gravedad en la valoración del riesgo que conlleva el uso de los sistemas y modelos de IA. La noción de “riesgo”, definida en dicha norma como “la combinación de la probabilidad de que se produzca un daño y la gravedad de dicho daño” (art. 3.2 del RIA), sirve de base para establecer una “pirámide de riesgos” ascendente (del riesgo medio/bajo hasta el riesgo inaceptable, pasando por el riesgo alto) que se emplea para clasificar una serie de prácticas y casos de uso de la IA en ámbitos específicos, lo que supone reconocer que no todos los tipos de IA suponen un riesgo y que no todos los riesgos son iguales o requieren las mismas medidas de mitigación. Por ello, y en recta correspondencia, el RIA crea un sistema de obligaciones, garantías y responsabilidades para todos los agentes que actúan dentro de este nuevo ecosistema (proveedores, fabricantes, responsables del despliegue y, en el sentido más amplio, afectados por el uso de estos sistemas). Se construye, de este modo, lo que venimos calificando como el “triángulo de oro” del RIA: aproximación desde el riesgo, garantías y responsabilidades”, MERCADER UGUINA, JESÚS R. “Los usos de alto riesgo en el ámbito laboral de la IA y la auto certificación”, *El foro de labos*, <https://www.elforodelabos.es/2024/05/los-usos-de-alto-riesgo-en-el-ambito-laboral-de-la-ia-y-la-autocertificacion/>.

De igual manera que en el Considerando 70 del Reglamento de IA se especifica que *“a fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben -con carácter excepcional, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas y tras la aplicación de todas las condiciones aplicables establecidas en el presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680- ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725”*.

Incluso en relación con los riesgos sistémicos ya prevé, Considerando 110: *“la capacidad de controlar sistemas físicos e interferir en el funcionamiento de infraestructuras críticas, a los riesgos derivados del hecho que los modelos hagan copias de sí mismos o se «autorrepliquen» o entrenen a otros modelos, a las maneras en que los modelos pueden dar lugar a sesgos dañinos y discriminación que entrañan riesgos para las personas, las comunidades o las sociedades, a la facilitación de la desinformación o el menoscabo de la intimidad, que suponen una amenaza para los valores democráticos y los derechos humanos, al riesgo de que un acontecimiento concreto dé lugar a una reacción en cadena con efectos negativos considerables que podrían afectar incluso a una ciudad entera, un ámbito de actividad entero o una comunidad entera”*.

Por todo ello regula en el artículo relativo a Datos y gobernanza de datos, artículo 10.2.f, que los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, entre otros, atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión.

De igual manera, artículo 10.5, *“en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes:*

a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

(...)

f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos”.

Por último, en su Anexo XI entre la información que deben presentar los proveedores de modelos de IA de uso general prevé una descripción de “*las especificaciones de diseño del modelo y el proceso de entrenamiento, incluidos los métodos y las técnicas de entrenamiento, las decisiones clave de diseño, incluidas la justificación lógica y los supuestos de los que se ha partido; aquello que el modelo está diseñado para optimizar y la pertinencia de los diversos parámetros, según proceda*”; y la “*información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y sus principales características; cómo se obtuvieron y seleccionaron los datos, así como cualquier otra medida que permita detectar que las fuentes de datos no son idóneas y los métodos para detectar sesgos identificables, cuando proceda*”.

En síntesis, el Reglamento de IA pone un gran énfasis en evitar que los sistemas de inteligencia artificial generen o perpetúen sesgos²⁵. Por ello, deben cumplir con unos requisitos destinados a asegurar su solidez técnica y eviten resultados sesgados que afecten desproporcionadamente a grupos marginados.

BIBLIOGRAFÍA

AGUIRRE SALA, JORGE FRANCISCO, “Especificando la responsabilidad algorítmica”, *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, Vol. 19, N.º. 2, 2022 (Ejemplar dedicado a: La educación digital en tiempo del COVID-19).

²⁵ Ya en las propuesta de Reglamento de 20 de octubre de 2020, contábamos con una Resolución centrada en las cuestiones éticas “Framework of ethical aspects of artificial intelligence, robotics and related technologies” 2020/2012(INL) , que incluía propuestas sobre cómo evitar sesgos y vulneración de los derechos fundamentales. Véase ÁLVAREZ OLALLA, PILAR, “Últimos trabajos pre-legislativos de la Unión Europea en Materia de Responsabilidad Civil por el uso de la Inteligencia Artificial”, en MUÑOZ VILLARREAL, ALBERTO (Dir.) *Derecho de los Riesgos Tecnológicos*, Eolas, 2021, pp. 163-199.

- ÁLVAREZ OLALLA, PILAR, “Últimos trabajos pre-legislativos de la Unión Europea en Materia de Responsabilidad Civil por el uso de la Inteligencia Artificial”, en MUÑOZ VILLARREAL, ALBERTO (Dir.) *Derecho de los Riesgos Tecnológicos*, Eolas, 2021, pp. 163-199.
- CÁMARA OUTES, AMANDA, *Responsabilidad civil de productos defectuosos de inteligencia Artificial*, 2023, ICEA-Universidad Pontificia de Salamanca.
- CORTINA ORTS, ADELA, “Ética de la inteligencia artificial”, *Anales de la Real academia de Ciencias Morales y Políticas* N. 96, 2019, pp. 379-394.
- FERNÁNDEZ SÁNCHEZ, SONIA, “Frank, el algoritmo consciente de Deliveroo. Comentario a la Sentencia del Tribunal de Bolonia 2949/2020, de 31 de diciembre”, *Revista de Trabajo y Seguridad Social*. CEF, 457 (abril 2021), pp. 179-193
- LAZCOZ MORATINOS, GUILLERMO y CASTILLO PARRILLA, JOSÉ ANTONIO “Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI”, *Revista Chilena de Derecho y Tecnología*, 2020, n. 1, pp. 207-225.
- LORENZO GÓNZALEZ, ANTONIO, *El derecho del trabajo ante la inteligencia artificial*, https://minerva.usc.es/xmlui/bitstream/handle/10347/30550/2022_LORENZO_Derecho_trabajo_inteligencia_artificial.pdf?sequence=1&isAllowed=y
- MERCADER UGUINA, JESÚS R. “Los usos de alto riesgo en el ámbito laboral de la IA y la auto certificación”, *El foro de labos*, <https://www.elforodelabos.es/2024/05/los-usos-de-alto-riesgo-en-el-ambito-laboral-de-la-ia-y-la-autocertificacion/>
- “Algoritmos y derecho del trabajo”, *Actualidad Jurídica* (1578- 956X), 2019, núm. 52, pp. 66-68.
- RIVAS VALLEJO, PILAR, “Sesgos de género en el uso de inteligencia artificial para la gestión de las relaciones laborales: análisis desde el derecho antidiscriminatorio”, *e-Revista Internacional de la Protección Social*, 2022, Vol. VII, N.º 1.
- SANTOS SÁNCHEZ, CLARA. *Los Algoritmos y el Derecho*, Facultad de Derecho de León, Inédito, 2021.
- TAPIA HERMIDA, ALBERTO, Sesgos y responsabilidades derivadas de la aplicación de la inteligencia artificial: el caso ChatGPT, <https://ajtapia.com/2023/04/sesgos-y-responsabilidades-derivadas-de-la-aplicacion-de-la-inteligencia-artificial-el-caso-chatgpt/>

Inteligencia artificial y responsabilidad civil: un enfoque ético en la era digital

IÑIGO A. NAVARRO MENDIZÁBAL

*Profesor Ordinario de Derecho Privado
Universidad Pontificia Comillas*

Sumario: 1. INTRODUCCIÓN. 2. PRINCIPIOS ÉTICOS DE LA IA. **2.1. La importancia de la Ética en la IA.** **2.2. Principales principios éticos.** 2.2.1. *Derechos Humanos y Dignidad.* 2.2.2. *Seguridad y Prudencia. Solidez y seguridad técnica.* 2.3. *Bienestar y Equidad. Diversidad e Inclusión.* 2.2.4. *Sostenibilidad.* 2.2.5. *Transparencia y Responsabilidad.* 3. INTENTO DE APORTAR SOLUCIONES A LOS DESAFÍOS A LOS QUE SE ENFRENTA LA TC POR DAÑOS CAUSADOS POR LA IA. **3.1. RC objetiva o subjetiva.** **3.2. La Explicabilidad y Opacidad de los Sistemas de IA (Black Box).** **3.3. Difusión de la Responsabilidad.** **3.4. Autonomía de la IA y Responsabilidad Humana.** **3.5. Daños colectivos y difusos.** **3.6. Daños futuros e inciertos.** 4. BIBLIOGRAFÍA

1. INTRODUCCIÓN

La inteligencia artificial (IA) ha dejado de ser ciencia ficción para convertirse en una realidad omnipresente en nuestra vida diaria¹. Desde asistentes virtuales y motores de búsqueda hasta sistemas avanzados de diagnóstico médico y vehículos autónomos, la IA está transformando la forma en que vivimos,

¹ Todo se está viendo afectado por la IA, desde el medio ambiente hasta nuestra propia mente como refleja la UNESCO: “Reconociendo las repercusiones positivas y negativas profundas y dinámicas de la inteligencia artificial (IA) en las sociedades, el medio ambiente, los ecosistemas y las vidas humanas, en particular en la mente humana, debido en parte a las nuevas formas en que su utilización influye en el pensamiento, las interacciones y la adopción de decisiones de los seres humanos», UNESCO, 2022, p.1.

trabajamos y tomamos decisiones. Este avance tecnológico trae consigo una serie de beneficios innegables, como el aumento de la eficiencia, la mejora de la precisión en diversas tareas y la capacidad de abordar problemas complejos que antes parecían insuperables.

Las ventajas de la IA las encontramos por todas partes². Pero la integración masiva de la IA en la sociedad también plantea importantes desafíos éticos y legales. A medida que los sistemas de IA adquieren mayor autonomía y capacidad de toma de decisiones, surgen preguntas críticas sobre de quién es la responsabilidad y la rendición de cuentas en caso de que algo salga mal. ¿Quién es responsable si un vehículo autónomo causa un accidente? ¿Qué sucede si un algoritmo de IA discrimina injustamente a un grupo de personas? Todo esto ha generado un momento que podríamos calificar como de reflexión adversativa: sabemos las ventajas de la IA, *pero...* tememos los inconvenientes, lo que genera inseguridad y a veces miedo³.

La ética para la IA no es solo una preocupación académica o teórica; es una necesidad práctica y urgente. La elaboración de principios éticos sólidos es crucial para garantizar que los sistemas de IA sean seguros, justos y transparentes. Los principios éticos, como el respeto a los Derechos Humanos y la

² Por ejemplo la Comisión Europea comenzaba su comunicación *Generar Confianza* diciendo: «La inteligencia artificial (IA) tiene potencial para transformar nuestro mundo para mejor: puede mejorar la asistencia sanitaria, reducir el consumo de energía, hacer que los vehículos sean más seguros y permitir a los agricultores utilizar el agua y los recursos de forma más eficiente. La IA puede utilizarse para predecir el cambio climático y medioambiental, mejorar la gestión del riesgo financiero y proporcionar las herramientas para fabricar, con menos residuos, productos a la medida de nuestras necesidades. La IA también puede ayudar a detectar el fraude y las amenazas de ciberseguridad y permite a los organismos encargados de hacer cumplir la ley luchar contra la delincuencia con más eficacia.

»La IA puede beneficiar a la sociedad y a la economía en su conjunto. Es una tecnología estratégica que se está desarrollando y utilizando a buen ritmo en todo el mundo. No obstante, también trae consigo nuevos retos para el futuro del trabajo y plantea cuestiones jurídicas y éticas», Comisión Europea, 2019, *Generar confianza*, p. 1.

³ Por ejemplo puede verse el Informe de Ipsos Global Views on AI (2023). De acuerdo con sus resultados, la consideración de las 3 afirmaciones que siguen fueron:

— Los productos y servicios que utilizan inteligencia artificial tienen más beneficios que inconvenientes (% de acuerdo muy/algo): 54% en global y 50% en España.

— Los productos y servicios que utilizan inteligencia artificial me emocionan (% de acuerdo muy/algo): 54 % en global y 50% en España.

— Los productos y servicios que utilizan inteligencia artificial me ponen nervioso (% de acuerdo(muy/algo)): 52% en global y 51% en España.

Resultados similares arrojó el estudio del Oxford Internet Institute (2020) *Global Attitudes Towards AI, Machine Learning & Automated Decision Making*. En sus conclusiones podemos leer: «*Internationally, sentiments about technology are ambivalent at best. There are important differences between which risks are most prominent in a particular country. For instance, North Americans and people from Western Europe see the development of AI and robotics as more likely harmful as beneficial. Survey respondents in South and East Asia are much more likely to see these developments as beneficial*».

dignidad de la persona, la seguridad y la prudencia, la solidez y la seguridad técnica, la búsqueda del bienestar y la equidad, promover la diversidad y la inclusión, la sostenibilidad y la exigencia de transparencia y responsabilidad, proporcionan un marco para guiar el desarrollo y la ejecución de la IA.

Estos principios ayudan a mitigar los riesgos asociados con la IA, como la posibilidad de errores, la perpetuación de sesgos y la falta de transparencia en la toma de decisiones. Además, promueven la confianza pública en las tecnologías de IA, lo que es esencial para su adopción generalizada y su integración exitosa en diversos ámbitos de la sociedad⁴.

Por otro lado es importante considerar que los avances tecnológicos son continuos, lo que nos genera a los juristas una cierta indeterminación, porque no sabemos si seremos capaces de ofrecer una respuesta adecuada a una realidad que mañana será diferente⁵. Sin duda los tiempos de los legisladores no se parecen en nada a los tiempos de los innovadores. Como advierten Floridi et al. (2018, p. 690), la IA es una fuerza poderosa, una nueva forma de agencia inteligente, que ya está remodelando nuestras vidas, nuestras interacciones y nuestros entornos y no una mera herramienta más que habrá que regular cuando esté madura.

La ética aplicada a la IA tiene una infinidad de áreas que abordar y miles de problemas que resolver, que pueden ir desde los daños individuales y sociales causados por la tecnología y la IA hasta el debate sobre cuál es el estatus moral de los sistemas de IA o sobre cómo deberíamos tratarla en el caso de que alguna vez tuviera autoconsciencia y sentimientos. Además, el análisis ético es exhaustivo y abarca desde los comportamientos humanos más directos que diseñan, construyen o utilizan la IA, hasta el comportamiento del propio sistema de IA que puede operar con mayor o menor autonomía respecto al usuario o al diseñador o fabricante del sistema. Además, a medida que el comportamiento de un sistema de IA se vuelve más impredecible, los problemas

⁴ Floridi et al. hablan de la ventaja de un enfoque ético «*On one side, ethics enables organisations to take advantage of the social value that AI enables*» y «*On the other side, ethics enables organisations to anticipate and avoid or at least minimise costly mistakes*», Floridi et al., 2018, p. 694.

Este enfoque dual, de forma más o menos parecida, se repite. Por ejemplo: «El objetivo de este enfoque ético es doble: por un lado, promover la concordancia o alineamiento entre las intenciones de las distintas partes y los valores éticos pertinentes para el uso previsto; por otro lado, identificar, corregir o denunciar las aplicaciones que sirven a fines éticamente inaceptables que ignoran, o violan, valores decisivos en relación con su ámbito de actuación», Llano Alonso, 2024, p. 188.

⁵ Como Susskind escribe muy gráficamente, no hay línea de llegada: «*what at once excites and unsettles me most is that there is no finishing line. No-one in Silicon Valley, China, or South Korea is dusting their hands off, proclaiming, 'job done'*», Susskind, 2019, p. 41.

éticos aumentan y la rendición de cuentas debe replantearse⁶, siendo también diferentes los problemas que plantean la IA específica y la IA general⁷.

En este contexto, el objetivo de este capítulo es explorar en profundidad la intersección entre la responsabilidad civil (RC) y los principios éticos de la IA cuando ésta causa daños. A través de un análisis detallado, pretende proporcionar una visión clara y comprensiva de cómo los principios éticos pueden y deben influir en la asignación de responsabilidad legal en casos de daños causados por la IA. También busca contribuir al debate académico y práctico sobre cómo manejar de manera efectiva los desafíos y oportunidades que presenta la IA. La combinación de un enfoque ético con una sólida base legal es esencial para asegurar que el avance tecnológico sea seguro, justo y equitativo para todos.

2. PRINCIPIOS ÉTICOS DE LA IA

2.1. LA IMPORTANCIA DE LA ÉTICA EN LA IA

Como señalaba la Comisión Europea (2019, p. 10) en su comunicación *Generar confianza*: «La dimensión ética de la IA no es un lujo ni un algo accesorio: ha de ser parte integrante del desarrollo de la IA. Al tratar de lograr una IA centrada en el ser humano basada en la confianza, salvaguardamos el respeto de los valores esenciales de nuestra sociedad y forjamos una marca distintiva para Europa y su industria como líder de la IA de vanguardia en la que se puede confiar en todo el mundo».

En esta misma comunicación, la Comisión Europea declara «La UE se asienta sobre un sólido marco normativo, que constituirá la referencia mundial para la IA centrada en el ser humano» convirtiendo a la UE en el principal regulador que además está sirviendo de inspiración para muchos otros países (efecto Bruselas)⁸.

⁶ Dignum, 2018, p. 1.

⁷ Se podría hablar de distintas aproximaciones al análisis ético de la IA, todos ellos necesarios (Dignum, 2018, p. 2):

- *"Ethics by Design: the technical/algorithmic integration of ethical reasoning capabilities as part of the behaviour of artificial autonomous system;*

- *Ethics in Design: the regulatory and engineering methods that support the analysis and evaluation of the ethical implications of AI systems as these integrate or replace traditional social structures;*

- *Ethics for Design: the codes of conduct, standards and certification processes that ensure the integrity of developers and users as they research, design, construct, employ and manage artificial intelligent systems".*

⁸ El concepto «efecto Bruselas» lo expuso Bradford analizando el impacto global del poder normativo de la UE y cómo sus regulaciones se extienden a nivel mundial sin necesidad de instituciones internacionales ni acuerdos de cooperación explícitos (Bradford, 2012).

La necesidad de una regulación basada en principios éticos es urgente en la UE, porque si no dictamos las reglas, nos serán dictadas⁹. Además es necesario que la regulación tenga el «enfoque europeo» basado en principios éticos¹⁰.

Dentro de esta importancia de la ética, Mittelstadt et al. (2016) en su interesante artículo *The ethics of algorithms: Mapping the debate*, elaboraron un mapa conceptual de las principales preocupaciones éticas que nos presentan los algoritmos que toman decisiones y que afectan a la sociedad y a los individuos. En el artículo se identifican:

A) Tres tipos de preocupaciones epistémicas:

1. La evidencia inconclusa: el conocimiento probable y a menudo incierto que producen los algoritmos puede llevar a acciones basadas en información insuficiente.
2. La evidencia inescrutable: la falta de transparencia en cómo los algoritmos generan conclusiones puede hacer que las decisiones sean difíciles de entender y escrutar.
3. La evidencia errónea de la IA cuando la calidad de las conclusiones de los algoritmos está limitada por la calidad de los datos de entrada.

B) Dos tipos de preocupaciones normativas:

1. Los resultados injustos cuando las acciones impulsadas por algoritmos pueden ser evaluadas según su justicia, afectando a ciertos grupos de manera desproporcionada.
2. Los efectos transformadores, porque los algoritmos pueden cambiar cómo conceptualizamos el mundo y reorganizar aspectos sociales y políticos.

C) La trazabilidad, que es una preocupación transversal y que está relacionada con la capacidad de asignar responsabilidad y rendir cuentas por los efectos de los algoritmos.

⁹ Reconoce el Parlamento Europeo: «si la Unión no actúa con rapidez y valentía, acabará teniendo que seguir las reglas y normas fijadas por otros y corre el riesgo de sufrir efectos perjudiciales para la estabilidad política, la seguridad social, los derechos fundamentales, las libertades individuales y la competitividad económica », Parlamento Europeo, 2020, *IA en la Era Digital*, 6.

¹⁰ «Pone de relieve que un objetivo subyacente a la estrategia digital de la Unión, así como al de la estrategia de la IA, es crear un «enfoque europeo» en un mundo digitalizado; aclara que este enfoque debe estar centrado en el ser humano, ser fiable, guiarse por principios éticos y basarse en el concepto de economía social de mercado; subraya que la persona y la protección de sus derechos fundamentales deben permanecer siempre en el centro de todas las consideraciones políticas», Parlamento Europeo, 2020, *IA en la Era Digital*, 130.

Quizás una de las cuestiones que muestra de manera clara la necesidad de la ética de la IA, es que los algoritmos toman decisiones por las personas. Así, pueden decidir tanto desde qué trayecto seguir para llegar al destino, qué restaurante visitar o con qué persona quedar para cenar, en el ámbito personal, como sobre cuestiones empresariales (inversiones, contrataciones entre muchas otras) gobernando cada vez más las empresas y las instituciones. Como señalan Mittelstadt et al. (2016, p. 1), «las operaciones, las decisiones y las opciones que antes se dejaban en manos de los seres humanos se delegan cada vez más en los algoritmos, que pueden aconsejar, si no decidir, sobre cómo deben interpretarse los datos y qué acciones deben adoptarse como resultado».

Pero además de esta “delegación de funciones”, cada vez es más difícil saber cómo toman las decisiones los algoritmos cuya incertidumbre y opacidad es cada vez más problemática¹¹. Ante esta capacidad de aprender de los algoritmos hay incluso quienes piensan que deben ser considerados agentes morales con una cierta responsabilidad moral¹².

La autonomía de la IA es una de las razones que impone con más fuerza la necesidad de una reflexión ética¹³, porque al poder adoptar decisiones sin un control humano directo, se puede perder el control ético generalmente atribuido a las personas. Esto está en el fondo de muchas de las distopías que se han bosquejado en la ciencia ficción y que podrían resumirse en la consideración de Bostrom y Yudkowsky (2014) según la cual una IA superinteligente, a menos que estuviera diseñada específicamente para actuar de manera beneficiosa para los humanos, podría perseguir sus propios objetivos de manera perjudicial para la humanidad, incluida la extinción humana¹⁴.

Muchos de estos temores gravitan en torno a las ideas de:

- La desalienación de objetivos entre los humanos y la IA¹⁵: «*The complexity of human values and the difficulty of embedding them correctly*

¹¹ Mittelstadt et al., 2016, p. 3.

¹² «*For some, learning algorithms should be considered moral agents with some degree of moral responsibility*», Mittelstadt et al., 2016, p.11.

Este debate no lo he tratado en este capítulo por múltiples razones, siendo una de las principales que en la UE se ha ido “desinflando” la idea de una posible RC de la IA o de los robots que tuvieran “personalidad digital” y se ha optado por la RC de personas tales como el fabricante.

¹³ «*Incorporating ethical principles into the design of AI systems is essential to ensure that their decision-making processes are transparent and that they can be audited and controlled effectively*», Bostrom y Yudkowsky, 2014.

¹⁴ «*A superintelligent AI, unless specifically designed to act in ways that are beneficial to humans, could pursue its own goals in ways that are harmful to humanity, including causing human extinction*», Bostrom y Yudkowsky, 2014.

¹⁵ Por ejemplo, estos miedos están relacionados con los principios 10 y 11 de los Principios Asilomar: «10) *Value Alignment: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation*» y «11) *Human Values: AI*

in a machine makes it likely that any simple goal given to an AI could result in unforeseen and potentially disastrous actions» (Bostrom y Yudkowsky, 2014)¹⁶.

- El miedo a la pérdida de control: *«Ensuring that an AI remains under human control is essential, as an uncontrolled AI could modify itself in ways that make it even more difficult to control, potentially leading to catastrophic outcomes»* (Bostrom y Yudkowsky, 2014).

La integración de los principios éticos en normativas y estándares es crucial para garantizar que las tecnologías de IA se desarrollen y utilicen de manera ética¹⁷. Quizás una argumentación poderosa que demuestra la necesidad de la ética en este campo sería la *reductio ad absurdum*, pues ¿qué pasaría si se desarrollara la IA sin ninguna cortapisa? Probablemente nos acercaríamos en mayor o menor grado a las distopías de la ciencia ficción. Podrían ocurrir cosas tales como:

- Amenazas a la seguridad tanto individual como colectiva. La IA podría usarse para fines maliciosos como el desarrollo sin control de armas autónomas o la manipulación masiva de la información para desestabilizar sociedades. Es más, la IA podría autónomamente actuar de manera impredecible y peligrosa si no respetara principios éticos, lo que podría llevar a graves amenazas para la seguridad global.
- Deshumanización. La IA que toma decisiones, si no tuviera un control ético se deshumanizaría, lo que podría suponer no respetar valores tales como la dignidad o los derechos fundamentales y llevar una pérdida de control que incluso podría poner en riesgo la existencia de la humanidad.
- Automatización de la injusticia, pues se podrían perpetuar o programar sesgos con el fin de que se tomaran decisiones discriminatorias en áreas tan sensibles como la justicia, el mercado laboral o bancario o la asignación de recursos.

systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity», Future of Life Institute, 2017.

¹⁶ Véase también Llano Alonso, 2024, pp. 184-187.

¹⁷ También existen otras opiniones alternativas como la de Müller que analizando el problema de la alineación de valores en la IA propone, más allá de intentar crear «máquinas morales», el enfoque de la «domesticación» con una analogía con la relación que los seres humanos tenemos con los animales no humanos: *«while nonhuman animals and AI agents are different in many ways, the fundamental approach with which we have “value-aligned” animals is transferable to AI agents, and can guide us in understanding how human moral agents can cooperate with nonhuman agents without human-like moral capabilities»*, Müller, 2022, p. 235.

- Neoludismo. Una IA sin ética también podría generar una masiva reacción en contra de la tecnología como un neoludismo debido a que se generaría una falta de confianza pública.

Muchos organismos internacionales han comenzado a adoptar marcos regulatorios y directrices para orientar el uso ético de la IA. Se pueden citar, como principales:

- **Directrices Éticas para una IA fiable**¹⁸: establece un marco normativo y ético para el desarrollo y uso de la IA en la UE. Estas directrices buscan garantizar que la IA sea confiable, segura y respetuosa con los derechos fundamentales y los valores europeos. Su importancia radica en promover un enfoque de la IA que no solo impulse la innovación, sino que también proteja a los individuos y la sociedad, fomentando la transparencia, la responsabilidad y la sostenibilidad en la adopción de estas tecnologías¹⁹.

¹⁸ Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial. (2019). *Directrices éticas para una IA fiable*. Comisión Europea.

Las Directrices Éticas para una IA Fiable fueron elaboradas por el Grupo Independiente de Expertos de Alto Nivel sobre IA, un comité creado por la Comisión Europea en 2018 (en la bibliografía y en las citas he considerado autor al Grupo, aunque el autor corporativo es la propia Comisión Europea). El proceso de elaboración de las directrices siguió un enfoque abierto, inclusivo y deliberativo y se pueden citar como momentos clave:

- creación del grupo de expertos: la Comisión Europea seleccionó a un grupo multidisciplinario de expertos procedentes de la academia, la industria y la sociedad civil. Estos expertos tenían conocimientos diversos en áreas como IA, derecho, filosofía, ética, y economía, asegurando una amplia representación de diferentes perspectivas;

- proceso de consulta pública que fue uno de los pilares de la elaboración: tras elaborar un borrador se abrió una consulta pública en la que ciudadanos, investigadores, ONGs, y empresas pudieron compartir sus opiniones y preocupaciones respecto a la IA y su desarrollo ético;

- revisión en varias fases con ajuste del documento tras los comentarios recibidos;

- publicación de la versión definitiva el 8 de abril de 2019.

¹⁹ Como se verá a lo largo del texto, considero que estas Directrices son una base fundamental dentro de la UE para hacer un análisis ético de la IA que sirva para fundamentar la regulación.

Esto no obstante, ha habido diversas posiciones críticas con este documento que en aras a la objetividad conviene citar. Por ejemplo Stamboliev y Christiaens consideran que el concepto de *Trustworthy AI* (IA Confiable) funciona como un «significante vacío», es decir, un término vago que busca unir a diferentes actores con intereses contradictorios, como la industria, los expertos en ética y los legisladores, si bien lo hacen tomando conceptos de la filosofía política de los filósofos postmarxistas Ernesto Laclau y Chantal Mouffe. Los autores del artículo destacan la subordinación de la ética a la industria tecnológica adoptando aquella el rol de un “extintor de incendios” para minimizar daños una vez que la tecnología está desarrollada. Entre los posibles escenarios futuros que plantean están: (i) *Status Quo*, en el que se mantiene el equilibrio frágil actual; (ii) *Asimilación*, donde la ética queda completamente absorbida por los intereses de la industria; y (iii) *Contestación*, en el que la ética desafía la hegemonía de la industria y toma un rol más crítico y autónomo (Stamboliev y Christiaens, 2024). Considero que quizás podríamos pensar en una asimilación con contestación, en la que la ética manteniendo una cierta independencia, se integrara en la regulación que la industria debe cumplir.

Este documento no es vinculante, pero, dentro del llamado «enfoque europeo»²⁰, proporciona un marco de referencia ético para el desarrollo de la IA dentro de la UE, basado en los valores fundamentales de la UE, tales como el respeto a los derechos humanos, la democracia, el Estado de derecho y el bienestar social. Pretende ser el pilar ético de la normativa, por lo que lógicamente influirá en futuras legislaciones y políticas sobre IA, por lo que es particularmente importante para nosotros.

- **Recomendación sobre la ética de la inteligencia artificial de la UNESCO**²¹: adoptada en 2021 establece principios y valores fundamentales para guiar el desarrollo y uso de la IA en todo el mundo: subraya la importancia de la dignidad humana, la sostenibilidad, la diversidad y la inclusión en la IA. Propone un marco ético que abarca desde la transparencia y la rendición de cuentas hasta la protección de datos y la equidad. Su objetivo es garantizar que la IA se desarrolle y aplique de manera que respete los derechos humanos y promueva el bienestar de todos, evitando cualquier tipo de discriminación o daño social. Esta recomendación es relevante porque ofrece una guía globalmente reconocida para la adopción responsable de la IA, influenciando políticas y prácticas a nivel internacional.
- **Principios de la OCDE sobre IA**²²: buscan promover un desarrollo y uso de la IA que sea innovador y responsable. Estos principios se centran en asegurar que la IA respete los derechos humanos, promueva el crecimiento inclusivo, sea transparente y explicable, y esté diseñada para funcionar de manera robusta y segura. Además, subrayan la importancia de la cooperación internacional y la necesidad de establecer marcos regulatorios que promuevan la confianza en la IA a nivel global. Su relevancia radica en la orientación que brindan a los gobiernos y las empresas para que el desarrollo de la IA se realice de manera ética y beneficie a la sociedad en su conjunto.
- **Principios de Asilomar para la IA**²³: son un conjunto de principios formulados en 2017 por expertos en IA, ética y tecnología durante una conferencia en Asilomar, California. Estos principios están diseñados

También ha habido críticas que acusan al documento de promover el *ethic washing*, como recoge Larsson (2020, p. 443).

²⁰ Parlamento Europeo, 2020, *IA en la Era Digital*, 130.

²¹ UNESCO. (2022). *Recomendación sobre la ética de la inteligencia artificial*. La Recomendación sobre la ética de la inteligencia artificial de la UNESCO fue adoptada por los 193 Estados Miembros de la Organización en noviembre de 2021.

²² OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

²³ Future of Life Institute. (2017). *Asilomar AI Principles*.

para garantizar que el desarrollo de la inteligencia artificial sea seguro, ético y beneficioso para la humanidad. Los principios incluyen pautas sobre la transparencia, la justicia, la responsabilidad y la alineación con los valores humanos, así como la necesidad de una investigación robusta y una cooperación internacional para mitigar los riesgos asociados con la IA avanzada. La importancia de los Principios de Asilomar radica en su enfoque proactivo para abordar los desafíos éticos y de seguridad que plantea la IA, promoviendo un desarrollo de la tecnología que sea responsable y alineado con los intereses del bienestar global.

- **Declaración de Montreal²⁴**: creada en 2018 por un grupo de académicos, expertos y miembros de la sociedad civil en Montreal, esta Declaración busca asegurar que la IA respete la dignidad humana, los derechos individuales y el bienestar colectivo. Los principios clave incluyen la transparencia, la equidad, la responsabilidad, la inclusión y la sostenibilidad. La carta también subraya la necesidad de que las decisiones automatizadas sean comprensibles y explicables, y que las tecnologías de IA se utilicen para el beneficio común, evitando sesgos y discriminaciones. Su importancia radica en ofrecer un marco ético que guíe a desarrolladores, empresas y gobiernos en la adopción de la IA de manera que promueva el respeto por los valores humanos y la justicia social.
- **Directrices del IEEE para un Diseño Ético de la IA²⁵**: recomendaciones desarrolladas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para orientar el diseño y la implementación de la IA y los sistemas autónomos. Estas directrices enfatizan la necesidad de integrar principios éticos desde las primeras etapas del desarrollo de la IA, promoviendo la protección de los derechos humanos, la privacidad, la equidad y la transparencia. También abordan cuestiones como la responsabilidad, la seguridad, y el impacto social de la tecnología. La importancia de estas directrices radica en su enfoque en crear sistemas de IA que no solo sean técnicamente robustos, sino también alineados con los valores éticos y las expectativas sociales, ayudando a minimizar los riesgos y maximizar los beneficios de la IA para todos los usuarios.

²⁴ Institut de Valorisation Des Données (IVADO). (2018). *Montreal Declaration for a Responsible Development of Artificial Intelligence*.

²⁵ IEEE. (2019). *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition*.

También hay muchísimas otras iniciativas como la *Guía de buenas prácticas en el uso de la IA ética de OdiseIA*²⁶ que proporciona directrices y recomendaciones para que las organizaciones y empresas implementen sistemas de IA de manera ética y responsable, siguiendo principios éticos y normativos²⁷.

2.2. PRINCIPALES PRINCIPIOS ÉTICOS

Como se ha visto son muchos los documentos que han tratado de buscar unos principios éticos para la IA partiendo de diferentes enfoques y/o analizando distintas áreas.

En este epígrafe se han analizado dichos documentos con el objetivo de extraer los principios éticos que deben gobernar la IA para aplicarlos posteriormente a la RC.

A continuación se presenta los principales:

2.2.1. Derechos Humanos y Dignidad

Que el respeto a los Derechos humanos y a la dignidad de la persona es un principio que debe ordenar el desarrollo y uso de la IA es una obviedad elemental que no habría ni que mencionar. Sin embargo, en muchos de los documentos que hemos aludido, aparece citado explícitamente como uno de los principios, por lo que conviene señalarlo (lo que abunda no daña reza el refranero español).

Más que un principio ético podría decirse que es el cimiento sobre el que se construye el resto de la arquitectura ética. Como señalan las Directrices

²⁶ OdiseIA, PwC, Google, Microsoft, IBM, y Telefónica. (2022). *Guía de buenas prácticas en el uso de la inteligencia artificial ética*.

²⁷ No faltan en la literatura opiniones que se muestran pesimistas en cuanto a la efectividad práctica de las guías éticas que se están desarrollando sobre la IA. Por ejemplo Hagendorff, en su trabajo *The Ethics of AI Ethics: An Evaluation of Guidelines*, realiza un análisis de 22 guías éticas sobre IA, poniendo en evidencia su limitada efectividad para influir en la toma de decisiones de los desarrolladores y la industria. A pesar de que estas guías formulan principios como la transparencia, la privacidad y la justicia, Hagendorff destaca la falta de mecanismos de aplicación reales que aseguren su cumplimiento. Este vacío, sostiene, permite a las empresas utilizar las guías como herramientas de relaciones públicas, desalentando la creación de un marco legal vinculante. Además, las guías tienden a centrarse en soluciones técnicas, mientras omiten cuestiones más amplias como los costos sociales y ecológicos, así como los riesgos de abuso político de la IA. Para mitigar estas deficiencias, el autor aboga por complementar las guías deontológicas con un enfoque basado en la ética de las virtudes, que fomente la responsabilidad moral en los desarrolladores. Estas reflexiones nos deben hacer pensar para fundamentar un marco de RC que exija rendición de cuentas ante posibles daños derivados del uso indebido o negligente de la IA, Hagendorff, 2020, pp. 99-120.

éticas para una IA fiable «El respeto de los derechos fundamentales, dentro de un marco de democracia y estado de Derecho, proporciona la base más prometedora para identificar los principios y valores éticos abstractos que se pueden poner en práctica en el contexto de la IA»²⁸.

Por otro lado también nos recuerda con claridad que la legalidad, el Derecho y la Ética no difieren cuando estamos en la realidad *offline* y *online*²⁹. En ocasiones parece que algunas personas no consideran de la misma manera lo que ocurre en el mundo digital y lo que pasa fuera de él, pero un daño moral o una filtración de datos que genere daños resarcibles se puede producir en un periódico tradicional, en Instagram o en X.

Dentro de este apartado se pueden señalar tres ejes:

A) Respeto de los Derechos humanos

Los sistemas de IA deben respetar y promover los derechos fundamentales, garantizando que su desarrollo y uso no vulnere la dignidad, las libertades y los derechos de las personas. Ejemplo de su formulación puede ser:

«La dignidad inviolable e intrínseca de cada ser humano constituye la base del sistema universal, indivisible, inalienable, interdependiente e interrelacionado de derechos humanos y libertades fundamentales. Por consiguiente, el respeto, la protección y la promoción de la dignidad humana y de los derechos establecidos por el derecho internacional, en particular el derecho internacional de los derechos humanos, son esenciales a lo largo del ciclo de vida de los sistemas de IA» (UNESCO, 2021, 13)³⁰.

²⁸ Grupo Independiente de Expertos, 2019, *Directrices éticas*, p. 12.

²⁹ Por ejemplo: «Los Estados Miembros deberían velar por que se investiguen y reparen los daños causados mediante sistemas de IA, estableciendo mecanismos de aplicación estrictos y medidas correctivas, a fin de asegurarse de que los derechos humanos, las libertades fundamentales y el estado de derecho son respetados en el mundo digital y en el mundo físico» (UNESCO, 2022, p. 55).

³⁰ Otras formulaciones:

- «*AI/IS should be designed and operated in a way that both respects and fulfills human rights, freedoms, human dignity, and cultural diversity*». (IEEE, 2019, Principle 1, p. 22).

- «*AI actors should respect the rule of law, human rights, democratic and human-centred values throughout the AI system lifecycle. These include non-discrimination and equality, freedom, dignity, autonomy of individuals, privacy and data protection, diversity, fairness, social justice, and internationally recognised labour rights. This also includes addressing misinformation and disinformation amplified by AI, while respecting freedom of expression and other rights and freedoms protected by applicable international law*», OECD, 2019, p. 8.

— Principios Asilomar: «(11) *Human Values: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity*», Future of Life Institute, 2017.

B) Respeto de la Autonomía humana

La IA debe permitir que las personas mantengan el control sobre sus decisiones y acciones en todos los ámbitos:

- «Las personas que interactúen con sistemas de IA deben poder mantener una autonomía plena y efectiva sobre sí mismas y ser capaces de participar en el proceso democrático. Los sistemas de IA no deberían subordinar, coaccionar, engañar, manipular, condicionar o dirigir a los seres humanos de manera injustificada. En lugar de ello, los sistemas de IA deberían diseñarse de forma que aumenten, complementen y potencien las aptitudes cognitivas, sociales y culturales de las personas. La distribución de funciones entre los seres humanos y los sistemas de IA debería seguir principios de diseño centrados en las personas, y dejar amplias oportunidades para la elección humana», Grupo Independiente de Expertos, 2019, *Directrices éticas*, 50, p. 15.
- «Los sistemas de IA deberían respaldar la autonomía y la toma de decisiones de las personas, tal como prescribe el principio del *respeto de la autonomía humana*. Esto requiere que los sistemas de IA actúen tanto como facilitadores de una sociedad democrática, próspera y equitativa, apoyando la acción humana y promoviendo los derechos fundamentales, además de permitir la supervisión humana», Grupo Independiente de Expertos, 2019, *Directrices éticas* 62, p. 19³¹.

C) Respeto de la privacidad e intimidad

La protección de la privacidad y la intimidad es esencial en el contexto de la IA. Este principio establece que los sistemas no deben invadir la vida privada ni recopilar datos sin un control estricto.

La privacidad de los datos personales debe ser protegida en todas las etapas del desarrollo y uso de sistemas de IA. Esto incluye la recopilación, almacenamiento y procesamiento de datos. Los desarrolladores deben implementar medidas de seguridad robustas y asegurar que los datos se utilicen de manera

³¹ Otras enunciaciones:

— Declaración de Montreal: «*AI must allow individuals to fulfill their own moral objectives and their conception of a life worth living*» (IVADO, 2018, Principio 2: Respeto a la Autonomía, p. 9).

— Principios Asilomar «13) *Liberty and Privacy: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty*».

— «16) *Human Control: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives*», Future of Life Institute, 2017.

ética y con el consentimiento informado de los individuos. Por ejemplo, los asistentes virtuales deben garantizar que las conversaciones privadas no se almacenen ni se compartan sin el consentimiento del usuario.

Ejemplo:

«La privacidad es un derecho fundamental que se ve especialmente afectado por los sistemas de IA, y que guarda una estrecha relación con el *principio de prevención del daño*. La prevención del daño a la privacidad también requiere una adecuada gestión de los datos, que abarque la calidad y la integridad de los datos utilizados, su pertinencia en contraste con el ámbito en el que se desplegarán los sistemas de IA, sus protocolos de acceso y la capacidad para procesar datos sin vulnerar la privacidad». (Directrices éticas para una IA fiable, 71, p. 21)³².

2.2.2. Seguridad y Prudencia. Solidez y seguridad técnica

Los sistemas de IA deben ser seguros y robustos, garantizando su correcto funcionamiento durante toda su vida útil, y deben prever mecanismos para minimizar riesgos. Los desarrolladores de IA deben anticipar posibles consecuencias negativas y tomar medidas para evitarlas³³, promoviendo un desarrollo seguro y controlado. Además, los sistemas de IA deben ser diseñados para minimizar los riesgos de mal uso o abuso, implementando salvaguardas apropiadas.

³² Otras exposiciones:

- Declaración de Montreal: «*Personal spaces in which people are not subjected to surveillance or digital evaluation must be protected from the intrusion of AIS and data acquisition and archiving systems (DAAS). The intimacy of thoughts and emotions must be strictly protected from AIS and DAAS uses capable of causing harm, especially uses that impose moral judgments on people or their lifestyle choices*» (IVADO, 2018, Principio 3: Protección de la Privacidad e Intimidad, p. 10).

- Principios Asilomar «12) *Personal Privacy: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data*», Future of Life Institute, 2017.

³³ Por ejemplo: «*Plan de repliegue y seguridad general*. Los sistemas de IA deberían contar con salvaguardas que posibiliten un plan de repliegue en el caso de que surjan problemas. Esto puede significar que los sistemas de IA pasen de un procedimiento basado en estadísticas a otro basado en normas, o que soliciten la intervención de un operador humano antes de proseguir con sus actuaciones.³⁹ Es preciso garantizar que el sistema se comportará de acuerdo con lo que se espera de él sin causar daños a los seres vivos ni al medio ambiente. Esto incluye la minimización de las consecuencias y errores imprevistos. Además, se deberían establecer procesos dirigidos a aclarar y evaluar los posibles riesgos asociados con el uso de sistemas de IA en los diversos ámbitos de aplicación. El nivel de las medidas de seguridad requeridas depende de la magnitud del riesgo que plantee un sistema de IA, que a su vez depende de las capacidades del sistema. Cuando se prevea que el proceso de desarrollo o el propio sistema planteará riesgos particularmente altos, es crucial desarrollar y probar medidas de seguridad de forma proactiva», Grupo Independiente de Expertos, 2019, *Directrices éticas*, 68.

«2. Solidez técnica y seguridad. 66) Un componente crucial de la IA fiable es la solidez técnica, que está estrechamente vinculada al *principio de prevención del daño*. La solidez técnica requiere que los sistemas de IA se desarrollen con un enfoque preventivo en relación con los riesgos, de modo que se comporten siempre según lo esperado y minimicen los daños involuntarios e imprevistos, evitando asimismo causar daños inaceptables. Lo anterior debería aplicarse también a los cambios potenciales en su entorno operativo o a la presencia de otros agentes (humanos y artificiales) que puedan interactuar con el sistema de manera contenciosa. Además, debería garantizarse la integridad física y mental de los seres humanos», (Directrices éticas para una IA fiable, 66, p. 20)³⁴.

2.2.3. Bienestar y Equidad. Diversidad e Inclusión

Los sistemas de IA deben contribuir al bienestar humano³⁵, mejorando la calidad de vida, la salud y las condiciones laborales, sin causar daño. **Priorizar el bienestar humano** debe ser un objetivo principal del diseño de la

³⁴ Otras expresiones:

- UNESCO: «Seguridad y protección 27. Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deberían ser evitados y deberían tenerse en cuenta, prevenirse y eliminarse a lo largo del ciclo de vida de los sistemas de IA para garantizar la seguridad y la protección de los seres humanos, del medio ambiente y de los ecosistemas. La seguridad y la protección de la IA se propiciarán mediante el desarrollo de marcos de acceso a los datos que sean sostenibles, respeten la privacidad y fomenten un mejor entrenamiento y validación de los modelos de IA que utilicen datos de calidad.», UNESCO, 2022, p. 10.

- Principios de Asilomar «*AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible*», (Future of Life Institute, 2017, Principio 6: Safety).

- Declaración de Montreal: «*Every person involved in AI development must exercise caution by anticipating, as far as possible, the adverse consequences of AIS use and by taking the appropriate measures to avoid them*», (IVADO, 2018, Principio 8: Prudencia, p. 15).

- OECD: «1.4. Robustness, security and safety a) *AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety and/or security risks.*

- b) *Mechanisms should be in place, as appropriate, to ensure that if AI systems risk causing undue harm or exhibit undesired behaviour, they can be overridden, repaired, and/or decommissioned safely as needed.*

- c) *Mechanisms should also, where technically feasible, be in place to bolster information integrity while ensuring respect for freedom of expression*», OECD, 2019, p. 9.

- IEEE: «*Mitigate risks and negative impacts, including misuse, as A/IS evolve as socio-technical systems. In particular by ensuring A/IS are accountable and transparent*», IEEE, 2019, p. 20.

³⁵ «*The principle of creating AI technology that is beneficial to humanity is expressed in different ways, but it typically features at the top of each list of principles. Montreal and IEEE principles both use the term 'well-being': for Montreal, 'the development of AI should ultimately promote the well-being of all sentient creatures'; while IEEE states the need to 'prioritize human well-being as an outcome in all system designs*», Floridi et al., 2018, p. 696.

IA, utilizando métricas ampliamente aceptadas para medir el impacto en la calidad de vida.

«Para ello, es necesario que los sistemas de IA se centren en las personas y se fundamenten en el compromiso de utilizarlos al servicio de la humanidad y del bien común, con el objetivo de mejorar el bienestar y la libertad de los seres humanos» (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 10, p. 5)³⁶.

La IA debe **promover la Equidad** y garantizar que sus beneficios se distribuyan de manera justa, reduciendo las desigualdades sociales y económicas, sin perpetuar sesgos o discriminaciones. El principio de equidad también implica que el desarrollo de la IA debe promover un crecimiento inclusivo y sostenible, asegurando la igualdad de oportunidades y acceso.

La justicia en la IA implica la equidad en la distribución de beneficios y riesgos, evitando cualquier forma de discriminación o sesgo. Los sistemas de IA deben ser diseñados y entrenados con datos diversos y representativos para asegurar que no favorezcan a ningún grupo en detrimento de otro. Por ejemplo, los algoritmos de contratación deben ser evaluados para garantizar que no discriminen a candidatos por motivos de género, raza o edad y que no se perpetúen o amplíen las desigualdades existentes. La justicia puede influir en la responsabilidad civil al requerir que los sistemas de IA no discriminen ni causen daños desproporcionados a grupos vulnerables.

«El desarrollo, despliegue y utilización de sistemas de IA debe ser equitativo. Pese a que reconocemos que existen muchas interpretaciones diferentes de la equidad, creemos que esta tiene tanto una dimensión sustantiva como procedimental. La dimensión sustantiva implica un compromiso de: garantizar una distribución justa e igualitaria de los beneficios y costes, y asegurar que las personas y grupos no sufran sesgos injustos, discriminación ni estigmatización. Si se

³⁶ Otras muestras:

Declaración de Montreal «*AIS must help individuals improve their living conditions, their health, and their working conditions*», IVADO, 2018, Principio 1: Bienestar, p. 8.

- Principios Asilomar «1) *Research Goal: The goal of AI research should be to create not undirected intelligence, but beneficial intelligence*», Future of Life Institute, 2017.

- IEEE: «*A/IS should prioritize human well-being as an outcome in all system designs, using the best available and widely accepted well-being metrics as their reference point*» IEEE, 2019, p. 241.

- OECD: «1.1. *Inclusive growth, sustainable development and well-being. Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people and the planet, such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, well-being, sustainable development and environmental sustainability*», OECD, 2019, p. 8.

pueden evitar los sesgos injustos, los sistemas de IA podrían incluso aumentar la equidad social. También se debería fomentar la igualdad de oportunidades en términos de acceso a la educación, los bienes los servicios y la tecnología. Además, el uso de sistemas de IA no debería conducir jamás a que se engañe a los usuarios (finales) ni se limite su libertad de elección. Asimismo, la equidad implica que los profesionales de la IA deberían respetar el principio de proporcionalidad entre medios y fines, y estudiar cuidadosamente cómo alcanzar un equilibrio entre los diferentes intereses y objetivos contrapuestos. La dimensión procedimental de la equidad conlleva la capacidad de oponerse a las decisiones adoptadas por los sistemas de IA y por las personas que los manejan, así como de tratar de obtener compensaciones adecuadas frente a ellas. Con este fin, se debe poder identificar a la entidad responsable de la decisión y explicar los procesos de adopción de decisiones», (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 52, pp. 15 y 16)³⁷.

La IA debe respetar y promover la **diversidad** cultural y social, evitando la homogeneización de comportamientos y opiniones, y asegurando que las diferencias sean respetadas³⁸. Además, el desarrollo de la IA debe ser **inclusivo**,

³⁷ Otros ejemplos:

- Declaración de Montreal: «*AIS development must produce social and economic benefits for all by reducing social inequalities and vulnerabilities*», IVADO, 2018, Principio 6: Equidad, p. 13.

- OECD: «*Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people and the planet, such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, well-being, sustainable development and environmental sustainability*», OCDE, 2019, p. 8.

³⁸ Hay que tener en cuenta que algunas de las tendencias de la IA deben ser analizadas con detenimiento. Por ejemplo, Colmenarejo et al. (2022, pp. 114-115) reflejan la tensión que existe, entre otras, entre la estandarización y la localización. A través de la armonización de estándares, los sistemas de IA podrían ser conformes con la normativa, lo que ayudaría a la certeza jurídica y sería bueno para el mercado único. Sin embargo, una estandarización demasiado rígida podría no captar adecuadamente las complejidades y peculiaridades locales de los distintos contextos socioculturales. Esto podría generar soluciones de “talla única” que no abordaran problemas específicos, como ciertas desigualdades o sensibilidades culturales que varían entre regiones.

Por el contrario, la localización implica adaptar los sistemas y las regulaciones de IA a los contextos específicos de cada área o comunidad. Este enfoque tiene el potencial de personalizar las regulaciones y requisitos éticos, lo que puede ser crucial para abordar desigualdades particulares o sesgos que afectan a una población determinada. La localización permitiría ajustar los sistemas de IA para que respeten las particularidades geográficas, culturales y económicas de una región. No obstante, un enfoque puramente localizado correría el riesgo de entrar en conflicto con los valores fundamentales europeos, como el mercado común y el derecho a la igualdad. Si cada país o región estableciera sus propios estándares, podría socavarse la uniformidad normativa y generar fragmentación, creando barreras para las empresas que desearan operar en múltiples jurisdicciones.

permitiendo la participación de comunidades diversas y garantizando que no existan sesgos o discriminaciones en los sistemas.

«Para hacer realidad la IA fiable, es preciso garantizar la inclusión y la diversidad a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial. Además de tener en cuenta a todos los afectados y garantizar su participación en todo el proceso, también es necesario garantizar la igualdad de acceso mediante procesos de diseño inclusivos, sin olvidar la igualdad de trato. Este requisito está estrechamente relacionado con el *principio de equidad*», (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 79, p. 23)³⁹.

2.2.4. Sostenibilidad

La IA debe desarrollarse de manera sostenible, asegurando que no comprometa los recursos del planeta ni contribuya al deterioro del medio ambiente. El impacto ambiental de los sistemas de IA debe ser minimizado, optimizando la eficiencia energética y reduciendo los residuos tecnológicos durante todo su ciclo de vida. Ejemplo:

«Una IA sostenible y respetuosa con el medio ambiente. Los sistemas de inteligencia artificial prometen ayudar a abordar algunas de las preocupaciones sociales más urgentes; no obstante, se debe garantizar que lo hagan del modo más respetuoso posible con el medio ambiente. En ese sentido, debería evaluarse en su integridad el proceso de desarrollo, despliegue y utilización de sistemas de IA, así como toda su cadena de suministro, a través, por ejemplo, de un examen crítico del

³⁹ Otras muestras:

- UNESCO: «Garantizar la diversidad y la inclusión. 19. El respeto, la protección y la promoción de la diversidad y la inclusión deberían garantizarse a lo largo del ciclo de vida de los sistemas de IA, de conformidad con el derecho internacional, en particular el derecho de los derechos humanos. Para ello se podría promover la participación activa de todas las personas o grupos, con independencia de su raza, color, ascendencia, género, edad, idioma, religión, opiniones políticas, origen nacional, étnico o social, condición económica o social de nacimiento, discapacidad o cualquier otro motivo» UNESCO, 2022, p. 8.

- Declaración de Montreal: «*AI development and use must not lead to the homogenization of society through the standardization of behavior and opinions*», IVADO, 2018, Principio 7: Diversidad e Inclusión, p. 14.

- OECD: «1.1. *Inclusive growth, sustainable development and well-being. Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people and the planet, such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, well-being, sustainable development and environmental sustainability*», OECD, 2019, p. 8.

uso de los recursos y del consumo de energía durante la formación, dando prioridad a las opciones menos perjudiciales. Se deberían promover medidas que garanticen el respeto del medio ambiente por parte de todos los eslabones de la cadena de suministro», (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 84, p. 24)⁴⁰.

2.2.5. Transparencia y Responsabilidad

A) Transparencia y Explicabilidad

Los sistemas de IA deben ser transparentes, lo que significa que su funcionamiento debe ser explicable y verificable por terceros, permitiendo auditorías que respalden su uso seguro y responsable.

La transparencia y la explicabilidad⁴¹ están unidos⁴² pues se refieren a la capacidad de los sistemas de IA para proporcionar explicaciones comprensibles sobre cómo y por qué se toman ciertas decisiones. La explicabilidad es crucial para la transparencia y la rendición de cuentas. Por ejemplo, en el ámbito financiero, los algoritmos que determinan la aprobación de préstamos deben poder explicar claramente los factores que influyeron en cada decisión.

⁴⁰ Otras citas:

- UNESCO: «Sostenibilidad. 31. El desarrollo de sociedades sostenibles depende del logro de un complejo conjunto de objetivos relacionados con distintas dimensiones humanas, sociales, culturales, económicas y ambientales. La llegada de las tecnologías de la IA puede beneficiar los objetivos de sostenibilidad o dificultar su consecución, dependiendo de la forma en que se apliquen en países con diferentes niveles de desarrollo. Por consiguiente, la evaluación continua de los efectos humanos, sociales, culturales, económicos y ambientales de las tecnologías de la IA debería llevarse a cabo con pleno conocimiento de las repercusiones de dichas tecnologías en la sostenibilidad como un conjunto de metas en constante evolución en toda una serie de dimensiones, como las que se definen actualmente en los Objetivos de Desarrollo Sostenible(ODS) de las Naciones Unidas», UNESCO, 2022, pp.10 y 11.

- Declaración de Montreal: «The development and use of AIS must be carried out so as to ensure a strong environmental sustainability of the planet», IVADO, 2018, Principio 10: Desarrollo Sostenible, p. 17.

⁴¹ «The addition of this principle, which we synthesise as 'explicability' both in the epistemological sense of 'intelligibility' (as an answer to the question 'how does it work?') and in the ethical sense of 'accountability' (as an answer to the question: 'who is responsible for the way it works?'), is therefore the crucial missing piece of the jigsaw when we seek to apply the framework of bioethics to the ethics of AI», Floridi et al., 2018, p. 700.

⁴² La explicabilidad está directamente relacionada con la transparencia y es uno de los campos de batalla desde el punto de vista ético. Por ejemplo O'Neil en su libro «*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*» aborda cómo los algoritmos y el big data pueden perpetuar y exacerbar las desigualdades sociales y llegar a amenazar la democracia y señala con claridad: «To protect ourselves, we need to create a regulatory structure for Big Data and algorithmic decisions, one that ensures fairness and transparency», O'Neil, 2016.

Ejemplos:

«4. Transparencia 75) Este requisito guarda una relación estrecha con el *principio de explicabilidad* e incluye la transparencia de los elementos pertinentes para un sistema de IA: los datos, el sistema y los modelos de negocio, Grupo Independiente de Expertos, 2019, *Directrices éticas*, 75, p. 22.

«77) *Explicabilidad*. La explicabilidad concierne a la capacidad de explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas asociadas (por ejemplo, las áreas de aplicación de un sistema de IA). La explicabilidad técnica requiere que las decisiones que adopte un sistema de IA sean comprensibles para los seres humanos y estos tengan la posibilidad de rastrearlas. Además, puede que sea necesario buscar un equilibrio entre la mejora de la explicabilidad de un sistema (que puede reducir su precisión) o una mayor precisión de este (a costa de la explicabilidad). Cuando un sistema de IA tenga un impacto significativo en la vida de las personas, debería ser posible reclamar una explicación adecuada del proceso de toma de decisiones del sistema de IA. Dicha explicación debería ser oportuna y adaptarse al nivel de especialización de la parte interesada (que puede ser una persona no experta en la materia, un regulador o un investigador). Además, debería ser posible disponer de explicaciones sobre la medida en que el sistema de IA condiciona e influye en el proceso de toma de decisiones de la organización, sobre las decisiones de diseño del sistema y sobre la lógica subyacente a su despliegue (garantizando así la transparencia del modelo de negocio)», Grupo Independiente de Expertos, 2019, *Directrices éticas*, 77, p. 22⁴³.

⁴³ Otras formulaciones:

- UNESCO: «Transparencia y explicabilidad 37. La transparencia y la explicabilidad de los sistemas de IA suelen ser condiciones previas fundamentales para garantizar el respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y los principios éticos. La transparencia es necesaria para que los regímenes nacionales e internacionales pertinentes en materia de responsabilidad funcionen eficazmente. La falta de transparencia también podría mermar la posibilidad de impugnar eficazmente las decisiones basadas en resultados producidos por los sistemas de IA y, por lo tanto, podría vulnerar el derecho a un juicio imparcial y a un recurso efectivo, y limita los ámbitos en los que estos sistemas pueden utilizarse legalmente» UNESCO, 2022, pp. 11 y 12.

- IEEE: «*Automated systems should generate audit trails recording the facts and law supporting decisions and such systems should be amenable to third-party verification to show that the trails reflect what the system in fact did. Audit trails should include a comprehensive history of decisions made in a case, including the identity of individuals who recorded the facts and their assessment of those facts. Audit trails should detail the rules applied in every mini-decision made by the system*», IEEE, 2019, p. 153.

- «Los conjuntos de datos y los procesos que dan lugar a la decisión del sistema de IA, incluidos los relativos a la recopilación y etiquetado de los datos así como a los algoritmos utilizados, deberían

B) Participación democrática

Este principio resalta la importancia de someter el desarrollo y uso de la IA al escrutinio democrático, promoviendo debates abiertos para garantizar que los sistemas sean justos y accesibles, por un lado, y, por otro, la IA no debe socavar los sistemas democráticos. Ejemplo:

«*Respeto de la democracia, la justicia y el estado de Derecho.* En las democracias constitucionales, todo poder gubernamental debe estar autorizado legalmente y limitado por la legislación. Los sistemas de IA deberían servir para mantener e impulsar procesos democráticos, así como para respetar la pluralidad de valores y elecciones vitales de las personas. Los sistemas de IA no deben socavar los procesos democráticos, las deliberaciones humanas ni los sistemas democráticos de votación. Asimismo, los sistemas de IA deben incluir un compromiso de garantizar que su funcionamiento no menoscabe los compromisos esenciales en los que se fundamenta el estado de Derecho -así como las leyes y reglamentos de obligado cumplimiento- y de asegurar el respeto de las garantías procesales y la igualdad ante la ley», (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 43, p. 13)⁴⁴.

C) Prevención del daño Rendición de cuentas y Responsabilidad

Aunque la IA pueda tomar decisiones, la responsabilidad final de las acciones derivadas de estas decisiones debe recaer siempre en los seres huma-

documentarse con arreglo a la norma más rigurosa posible con el fin de posibilitar la trazabilidad y aumentar la transparencia, Grupo Independiente de Expertos, 2019, *Directrices éticas*, p. 22).

- OECD: «1.3. *Transparency and explainability.* AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

i. to foster a general understanding of AI systems, including their capabilities and limitations,
 ii. to make stakeholders aware of their interactions with AI systems, including in the workplace,
 iii. where feasible and useful, to provide plain and easy-to-understand information on the sources of data/input, factors, processes and/or logic that led to the prediction, content, recommendation or decision, to enable those affected by an AI system to understand the output, and,

iv. to provide information that enable those adversely affected by an AI system to challenge its output», OECD, 2019, pp. 8 y 9.

- Principios Asilomar «7) *Failure Transparency:* If an AI system causes harm, it should be possible to ascertain why»

- «8) *Judicial Transparency:* Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority» Future of Life Institute, 2017.

⁴⁴ Otra versión: «AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate, and controls», (IVADO, 2018, Principio 5: Participación Democrática, p. 12).

nos. Los desarrolladores y operadores de IA deben ser responsables y rendir cuentas de los sistemas que crean, asegurando que puedan responder por sus efectos y decisiones. Además debe existir un sistema eficaz de responsabilidad para indemnizar a las víctimas por los daños que los sistemas de IA pudieran causar. Hay que recordar que no dañar es un principio ético esencial. Ya lo era en las Leyes de la Robótica⁴⁵ que imaginó Isaac Asimov, y que son citadas expresamente por las Normas de Derecho Civil sobre Robótica⁴⁶.

Ejemplos:

«7. Rendición de cuentas 87) Los requisitos anteriores se complementan con el de rendición de cuentas, estrechamente relacionado con el *principio de equidad*. Este requisito exige establecer mecanismos que permitan garantizar la responsabilidad y rendición de cuentas sobre los sistemas de IA y sus resultados, tanto antes de su implantación como después de esta» Grupo Independiente de Expertos, 2019, *Directrices éticas*, 87, p. 22.

«91) *Compensaciones*. Cuando se produzcan efectos adversos injustos, deberían preverse mecanismos accesibles que aseguren una compensación adecuada. El hecho de saber que se podrá obtener una reparación si las cosas no salen según lo previsto es crucial para garantizar la confianza. Se debería prestar atención a las personas o grupos vulnerables», Grupo Independiente de Expertos, 2019, *Directrices éticas*, 91⁴⁷.

⁴⁵ «(1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. (2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws».

⁴⁶ Parlamento Europeo, 2017, *Normas de Derecho civil*.

⁴⁷ Otras explicaciones:

- UNESCO: «68. Los Estados Miembros deberían elaborar, examinar y adaptar, según proceda, marcos reguladores para alcanzar la rendición de cuentas y la responsabilidad por el contenido y los resultados de los sistemas de IA en las diferentes etapas de su ciclo de vida. Cuando sea necesario, los Estados Miembros deberían introducir marcos de responsabilidad o aclarar la interpretación de los marcos existentes para garantizar la atribución de la responsabilidad por los resultados y el funcionamiento de los sistemas de IA. Además, al elaborar los marcos reguladores, los Estados Miembros deberían tener en cuenta, en particular, que la responsabilidad y la rendición de cuentas deben recaer siempre en última instancia en personas físicas o jurídicas y que no se debe otorgar personalidad jurídica a los propios sistemas de IA. Para lograrlo, esos marcos reguladores deberían ajustarse al principio de la supervisión humana y establecer un enfoque global centrado en los actores de la IA y los procesos tecnológicos que intervienen en las diferentes etapas del ciclo de vida de los sistemas de IA», UNESCO, 2022, 68, pp. 17 y 18.

- Declaración de Montreal: «Only human beings can be held responsible for decisions stemming from recommendations made by AIS, and the actions that proceed therefrom», IVADO, 2018, Principio 9: Responsabilidad, p. 16.

3. INTENTO DE APORTAR SOLUCIONES A LOS DESAFÍOS A LOS QUE SE ENFRENTA LA RC POR DAÑOS CAUSADOS POR LA IA

La RC en el contexto de la IA plantea varios desafíos cuando se consideran los principios y documentos éticos que hemos revisado. A continuación se identifican algunos de los más importantes.

En las siguientes páginas se ofrece una opinión sobre la posible solución a los mismos desde los principios éticos analizados. Nótese que los aportes realizados se basan en los principios éticos, con la intención de enriquecer el debate, sin entrar en otros aspectos.

3.1. RC OBJETIVA O SUBJETIVA

Una de las cuestiones que siempre aparece en primer lugar cuando se trata sobre la RC en materia de IA es cuál debe ser su naturaleza: objetiva o subjetiva⁴⁸.

Los documentos y principios éticos revisados proporcionan orientación sobre cómo enfrentar esta cuestión, pero no ofrecen una respuesta directa sobre si la RC debe ser subjetiva u objetiva. Aun así, ayudan a orientar la decisión.

En este sentido y a sabiendas de que existen muchísimos más factores que pueden influir en la decisión que se adopte (factores económicos, sociológicos, de mercado, geoestratégicos...), a partir de los principios éticos señalados anteriormente, se pueden realizar una serie de consideraciones:

- OECD: «1.5. Accountability a) AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of the art.

b) To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outputs and responses to inquiry, appropriate to the context and consistent with the state of the art.

c) AI actors, should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on an ongoing basis and adopt responsible business conduct to address risks related to AI systems, including, as appropriate, via co-operation between different AI actors, suppliers of AI knowledge and AI resources, AI system users, and other stakeholders. Risks include those related to harmful bias, human rights including safety, security, and privacy, as well as labour and intellectual property rights», OECD, 2019, p. 9.

- IEEE: «Lawmakers and enforcers need to ensure that the implementation of A/IS is not abused by businesses and entities employing the A/ IS to avoid liability or payment of damages. Governments should consider adopting regulations requiring insurance or other guarantees of financial responsibility so that victims can recover damages for harm that A/ IS cause», IEEE, 2019, p. 155.

- «Objective: Provide effective regulation of A/IS to ensure public safety and responsibility while fostering a robust AI industry», IEEE, 2019, p. 188.

⁴⁸ Velasco Perdigones, 2021.

- 1) La insistencia de los documentos en la **transparencia y explicabilidad** exige que la IA fiable y éticamente buena tenga la «capacidad de explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas asociadas (por ejemplo, las áreas de aplicación de un sistema de IA)»⁴⁹. Esta repetición de la transparencia podría hacernos pensar en una **RC subjetiva**, pues si fuera posible rastrear y explicar de dónde procede el daño que la IA ha causado, lo lógico sería atribuir la culpa y la RC al actor humano responsable de la acción u omisión que ha ocasionado el daño (que podría ser el fabricante, el diseñador, el operador...).
- 2) De forma parecida los principios de **autonomía humana** y de control humano siempre conducen a que exista una responsabilidad humana (recordemos ideas como: «*Only human beings can be held responsible for decisions stemming from recommendations made by AIS, and the actions that proceed therefrom*»⁵⁰). Si en el tipo de IA que queremos siempre hay una persona que es responsable, parecería lógico entender que ese responsable lo fuera también civilmente, lo que podría encajar mejor con una **RC subjetiva**.
- 3) Diferente resultado podría arrojar el análisis si se consideraran otros otros principios como los de **seguridad y prudencia, solidez y seguridad técnica**. El enfoque en la prevención y en la robustez técnica nos haría pensar que, aunque no se pudiera identificar la culpabilidad de un actor humano (lo que supondría que han fracasado los principios anteriormente citados), las víctimas deberían tener derecho a una compensación por los daños que hubieran sufrido, lo que nos llevaría a una **RC objetiva** pues se indemnizaría con independencia de poder atribuir una negligencia a un actuar humano.
- 4) Algo parecido ocurre si se tuvieran en cuenta los principios de **prudencia** o la **prevención del daño**. Es verdad que estos principios guían la actuación ex ante, pues buscan anticipar posibles consecuencias negativas y mitigar el mal uso, lo que podría llevar aparejado que debería exonerarse de responsabilidad a quien ha actuado con prudencia y prevención extremando su deber de cuidado, pero por otro lado, ante daños que son de naturaleza impredecible (fuera de la posible prevención), resultaría injusto exigir la prueba de la negligencia y la **RC objetiva** sería una solución más pragmática.

⁴⁹ Grupo Independiente de Expertos, 2019, *Directrices éticas*, 77, p. 22.

⁵⁰ IVADO, 2018, Principio 9: Responsabilidad, p. 16.

La RC subjetiva requiere la prueba de la culpa del causante del daño: la acción u omisión de la que trae causa el daño (que la realizó el fabricante, desarrollador, operador, usuario...) es negligente. Para poder operar en esta materia se necesita que el mal funcionamiento o uso indebido de la IA pueda ser explicado y atribuido a errores humanos. Sin embargo, tal nivel de explicabilidad no siempre es posible en sistemas de *deep learning* donde el comportamiento de los algoritmos puede presentarse de manera opaca y por ello resulte imposible averiguar y probar la culpa.

Hasta el concepto de culpa se está viendo trastocado con la IA⁵¹. Cuando una IA se equivoca no es fácil saber si ha sido negligente, porque no existe un estándar de diligencia que les sea aplicable⁵². Si se piensa en la diligencia de la persona que usa la IA, también hay cambios porque ahora una persona razonable como estándar de diligencia será una persona que usa IA⁵³.

Por su parte, para la RC objetiva basta con probar el daño y que este deriva causalmente de la actividad de la IA, aunque no se pueda precisar con una concreción exhaustiva el momento exacto del que deriva el comportamiento dañoso posterior. Por esta razón, la RC objetiva parece más aconsejable de acuerdo con los principios de seguridad y prevención del daño pues facilita la compensación a las víctimas que han sufrido daños, sobre todo si los principio de transparencia y explicabilidad no se han cumplido todo lo que debían.

De resultas de lo anterior, y aun siendo cuestionable, considero que la RC objetiva es más acorde con todos los textos que se refieren a los principio éticos de la IA. En todos ellos es habitual señalar la responsabilidad de los desarrolladores y operadores de la IA, aunque sea difícil la prueba de la negligencia en sistemas tecnológicos tan complejos. La RC objetiva sería coherente con los principios de equidad, seguridad y prevención del daño entre otros. La RC subjetiva, por su parte, podría servir para azuzar la búsqueda de la di-

⁵¹ Los retos que la IA supone para el concepto de negligencia se pueden ver en Selbst, 2020.

⁵² Como señala Borghetti: «*When one tries to assess the existence of a human fault or negligence, one always compares the behavior of the defendant with the one which a model human being would have adopted in the same circumstances. Such a comparison is valid and pertinent because we assume that all human beings share the same kind of rationality and should be able to figure out what is reasonable in any kind of circumstances. The problem is that algorithms do not function the way human beings do, and the outcomes they produce may not be the product of a human-like rationality. Besides, two algorithms designed to perform the same tasks might function along different types of rationality and may therefore face one same situation in very different ways*», Borghetti, 2019, 94-102.

⁵³ «*For example, once self-driving cars become safer than traditional vehicles, a jury might find that it is unreasonable to drive yourself rather than to use a self-driving car. Applying the "reasonable person using an autonomous computer" standard to the earlier hypothetical involving a child running into the street, the human driver's negligence would not be based on failing to stop in 100 feet as a self-driving car would have; rather, liability would be based on her driving in the first place. A reasonable person would not have driven*», Abbott, 2018, 37.

ligencia en todos los actores y para hacer responsables a los negligentes en aquellos casos en los que se pueda probar⁵⁴.

En cualquier caso, saber si conviene una RC objetiva o subjetiva es una duda que actualmente está instalada en los legisladores europeos. El art. 5 de la Propuesta de Directiva sobre responsabilidad en materia de IA impone que «la Comisión revisará la aplicación de la presente Directiva y presentará un informe al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, acompañado, en su caso, de una propuesta legislativa». En dicho informe «En particular, deberá evaluar la idoneidad de las normas de responsabilidad objetiva (sin culpa) para las demandas contra los operadores de determinados sistemas de IA -siempre que estas no estén ya reguladas por otras normas de responsabilidad de la Unión- y la necesidad de aseguramiento, teniendo en cuenta al mismo tiempo el efecto y el impacto en la introducción general y la adopción de los sistemas de IA, especialmente para las pymes»⁵⁵.

3. 2. LA EXPLICABILIDAD Y OPACIDAD DE LOS SISTEMAS DE IA (BLACK BOX)

Uno de los desafíos más significativos de la RC en esta materia es la opacidad o la falta de explicabilidad en los sistemas de IA, especialmente en tecnologías como las que incorporan procesos de *deep learning*. Los sistemas de IA pueden tomar decisiones basadas en complejos algoritmos que no siempre son comprensibles para los seres humanos. En estos casos, si el sistema de IA actúa de manera autónoma y no se puede explicar cómo llegó a una decisión o a causar un daño⁵⁶, puede ser extremadamente difícil identificar a

⁵⁴ Desde un punto de vista fundamentalmente jurídico véanse los argumentos muy interesantes y proclives a la RC subjetiva que propone Atienza Navarro, 2023, 12, 3.2 y 3.3.

⁵⁵ Conviene también recordar la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA de 2020, en cuyo Considerando 14 se decía «Reconoce que el tipo de sistema de IA sobre el que el operador ejerce control es un factor determinante en lo que respecta a la responsabilidad; observa que un sistema de IA que conlleve un alto riesgo inherente y actúe de manera autónoma potencialmente pone en peligro en mucha mayor medida al público en general; considera que, habida cuenta de los retos jurídicos que plantean los sistemas de IA para los regímenes de responsabilidad civil existentes, parece razonable establecer un régimen común de responsabilidad objetiva para los sistemas de IA autónomos de alto riesgo; subraya que este enfoque basado en el riesgo, que puede incluir varios niveles de riesgo, debe fundamentarse en criterios claros y una definición adecuada de riesgo elevado, así como ofrecer seguridad jurídica». Efectivamente, en el art. 4 se establecía una RC objetiva para los sistemas de IA de alto riesgo y en el art. 8 una RC subjetiva par los demás sistemas de IA.

⁵⁶ Benhamou y Ferland explican este efecto: «AI's designers do not program all the possible scenarios in advance, nor give specific instructions for each of them; rather, they set a goal for the machine and let AI process the data input, learn from it, and decide the best course of action to reach its goal. This leads to the scenario where the AI's programmers may not have exact understanding of how it reached such goal or what the stages leading to

un responsable o determinar si hubo negligencia. No se trata de algo aislado, sino de algo común que suele denominarse como el efecto “caja negra”⁵⁷. La opacidad es un obstáculo tanto para la RC subjetiva, como para la RC objetiva, porque afecta al nexo causal imprescindible en ambas para atribuir la RC⁵⁸.

La opacidad afecta además a la investigación y desarrollo de la IA, lo que también pone en entredicho el principio de participación democrática⁵⁹.

Es verdad que una de las exigencias éticas expuesta en los documentos analizados es la transparencia y explicabilidad, pero es que ni siquiera es técnicamente posible en todas las aplicaciones de la IA. Por otro lado, es también común afirmar que la responsabilidad siempre debe recaer en persona físicas o jurídicas que sean legalmente responsables⁶⁰. No podemos olvidar que des-

success were; in other words, they cannot explain the AI's “thought process” leading to the final result. The same is true for AI's failures which cannot always be explained or understood by humans. For instance, algorithms in precision medicine process patient and hospital data to predict patient risks and formulate diagnoses, but it is not always possible to identify which data elements were processed, the weight that was given to each element in the global assessment and whether there are unethical bias in the processing. Even in cases where the algorithm itself is rather simple, the data fed into the algorithm may be so diverse and ever changing (in the case of autonomous vehicles, one may think about inputs from cameras, sensors, lasers, microphones, etc.) that it is often impossible to reproduce the environment in which the injury happened and identify its source», Benhamou y Ferland, 2021, 8.

⁵⁷ «Que una aplicación que se apoye en la IA actúe de manera autónoma quiere decir que lleva a cabo una tarea sin que cada paso esté predefinido y que lo hace con menos o, en última instancia, sin ningún control o supervisión humanos inmediatos. Los algoritmos basados en el aprendizaje automático de la máquina pueden ser difíciles, si no imposible, de comprender («efecto caja negra»)), Comisión Europea, 2020, *Informe sobre las repercusiones*, p. 18.

⁵⁸ «La transparencia es necesaria para que los regímenes nacionales e internacionales pertinentes en materia de responsabilidad funcionen eficazmente» (UNESCO, 2022, 37).

⁵⁹ «From a regulatory standpoint, some of the most problematic features of AI are not features of AI itself, but rather the manner in which AI R&D work can be done. Discreetness refers to the fact that AI development work can be conducted with limited visible infrastructure. Diffuseness means that the individuals working on a single component of an AI system might be located far away from one another. A closely related feature, discreteness, refers to the fact that the separate components of an AI system could be designed in different places and at different times without any conscious coordination. Finally, opacity denotes the possibility that the inner workings of an AI system may be kept secret and may not be susceptible to reverse engineering. Each of these features is shared, to varying degrees, by R&D work on many technologies in the Information Age, but they present particularly unique challenges in the context of AI», Scherer, 2016, 370.

⁶⁰ Véase por ejemplo: «Los Estados Miembros deberían velar por que siempre sea posible atribuir la responsabilidad ética y jurídica, en cualquier etapa del ciclo de vida de los sistemas de IA, así como en los casos de recurso relacionados con sistemas de IA, a personas físicas o a entidades jurídicas existentes. La supervisión humana se refiere, por tanto, no solo a la supervisión humana individual, sino también a la supervisión pública inclusiva, según corresponda» (UNESCO, 2022, p. 35).

«Los Estados Miembros deberían elaborar, examinar y adaptar, según proceda, marcos reguladores para alcanzar la rendición de cuentas y la responsabilidad por el contenido y los resultados de los sistemas de IA en las diferentes etapas de su ciclo de vida. Cuando sea necesario, los Estados Miembros deberían introducir marcos de responsabilidad o aclarar la interpretación de los marcos existentes para garantizar la atribución de la responsabilidad por los resultados y el funcionamiento de los sistemas de IA. Además, al elaborar los marcos reguladores, los Estados Miembros deberían tener en cuenta, en particular, que la responsabilidad y la rendición de cuentas deben recaer siempre

de un punto de vista jurídico la imprevisibilidad de la IA ha sido programada y por tanto prevista por los diseñadores⁶¹.

En lo que toca a la explicabilidad, no se trata de optar entre una solución u otra, sino de buscar posibles respuestas para reducir o intentar eliminar la opacidad. Diversas posibilidades, no exhaustivas, pueden ser:

1. Reforzar la trazabilidad y la explicabilidad. Los propios sistemas de IA deberían incorporar mecanismos de trazabilidad y explicabilidad que permitieran rastrear las decisiones de la IA. Se trataría de procedimientos parecidos a lo que se denomina en el mundo de la aviación como “caja negra” y que es un registro de vuelo en el que se almacenan datos importantes de lo que acontece durante el vuelo para poder averiguar posteriormente lo que ha pasado.

Conviene recordar que el principio de transparencia está directamente relacionado con la prevención del daño, la rendición de cuentas y la responsabilidad. Mecanismos que favorecieran la trazabilidad y la explicabilidad favorecerían la audatibilidad de tal manera que sería más comprensible la comprensión del comportamiento de la IA para los usuarios, para los reguladores y para todas las personas afectadas. Sin duda también favorecería la prueba de la relación causal en los procedimientos de RC.

2. Desarrollar herramientas de certificación y auditorías independientes. Además de los mecanismo internos de la IA que favorezcan la explicabilidad, sería conveniente el desarrollo de auditorías independientes que permitieran analizar y verificar el comportamiento de los sistemas de IA.

Antes de comercializar o implementar un sistema de IA, este debería pasar por un proceso de **certificación** que asegurara que cumple con los estándares de seguridad, transparencia y explicabilidad establecidos en los principios éticos⁶².

en última instancia en personas físicas o jurídicas y que no se debe otorgar personalidad jurídica a los propios sistemas de IA. Para lograrlo, esos marcos reguladores deberían ajustarse al principio de la supervisión humana y establecer un enfoque global centrado en los actores de la IA y los procesos tecnológicos que intervienen en las diferentes etapas del ciclo de vida de los sistemas de IA» (UNESCO, 2022, p. 68).

⁶¹ «Thus, a learning AI's designers will not be able to foresee how it will act after it is sent out into the world - but again, such unforeseeable behavior was intended by the AI's designers, even if a specific unforeseen act was not», Scherer, 2016, pp. 36-37.

⁶² Señalan las Directrices éticas: «Dado que no cabe esperar que todas y cada una de las personas comprendan plenamente el funcionamiento y los efectos de los sistemas de IA, puede tenerse en consideración a aquellas organizaciones que puedan acreditar ante el público que un sistema de IA es transparente, responsable y equitativo. Estas certificaciones aplicarían normas desarrolladas para diferentes ámbitos de aplicación y técnicas de IA, convenientemente alineadas con las normas industriales y sociales del contexto específico de que se trate. », Grupo Independiente de Expertos, 2019, *Directrices éticas*, 107.

Los sistemas de IA deberían estar sujetos a auditorías periódicas que verificaran su funcionamiento y permitieran la trazabilidad de las decisiones que toman. Si se produce un daño, la auditoría permitiría identificar en qué punto del proceso ocurrió el fallo, facilitando así la determinación de responsabilidad⁶³.

En la misma línea podrían explorarse sistemas de certificación y auditoría que incluyeran estándares técnicos que garantizaran que los sistemas de IA puedan ser comprendidos y cumplen con los principios de transparencia y explicabilidad.

3. Considerar la **RC objetiva** mitigaría parcialmente los efectos negativos de la opacidad. Al no exigir la prueba de la negligencia y bastar con demostrar la relación de causalidad, la opacidad tendría menos campo de juego. Esto alinearía la RC objetiva con los principios de seguridad, prudencia, rendición de cuentas y garantizaría mejor la compensación de las víctimas que también es una idea que aparece, por ejemplo, en las Directrices éticas (Grupo Independiente de Expertos, 2019, *Directrices éticas*, 91, p. 25).

4. **Introducir la obligación de exhibición de prueba y presunciones.** La Propuesta de Directiva sobre responsabilidad en materia de IA establece normas sobre la exhibición de pruebas en los procesos de RCE por los daños causados por sistemas de IA de alto riesgo y sobre la carga de prueba en la RCE subjetiva por daños causados por sistemas de IA. Una de las razones importantes para introducir estos mecanismos es intentar contrarrestar el efecto caja negra:

«Las características específicas de la IA, incluidas su complejidad, su autonomía y su opacidad (el denominado efecto de «caja negra»), pueden dificultar o hacer excesivamente costoso para las víctimas determinar cuál es la persona responsable y probar que se cumplen los requisitos para una demanda de responsabilidad civil admisible. En particular, al reclamar una indemnización, las víctimas podrían tener que soportar unos costes iniciales muy elevados y enfrentarse a procedimientos judiciales mucho más largos, en comparación con los casos sin relación alguna con la inteligencia artificial. Por lo tanto, las víctimas

⁶³ «La auditabilidad es la capacidad para evaluar los algoritmos, los datos y los procesos de diseño.

Esto no implica necesariamente que siempre deba disponerse de forma inmediata de la información sobre los modelos de negocio y la propiedad intelectual del sistema de IA. La evaluación por parte de auditores internos y externos y la disponibilidad de los correspondientes informes de evaluación pueden contribuir a la fiabilidad de esta tecnología. En aplicaciones que afecten a los derechos fundamentales, incluidas las aplicaciones esenciales desde el punto de vista de la seguridad, los sistemas de IA deberían poder someterse a auditorías independientes», Grupo Independiente de Expertos, 2019, *Directrices éticas*, 88.

pueden verse disuadidas de intentar siquiera obtener una indemnización», Exposición de Motivos de la Propuesta de Directiva sobre responsabilidad en materia de IA.

Tanto la exhibición de prueba obligatoria, como las presunciones de causalidad son herramientas que están acordes con los principios de prevención del daño y responsabilidad para los supuestos en los que la transparencia y la explicabilidad no se han podido alcanzar.

5. Fomentar la supervisión humana. La supervisión humana es un principio que aparece en numerosos documentos y precisamente coadyuvaría a facilitar la transparencia y explicabilidad de la IA. En la medida en que un sistema de IA este sometido a un control humano y exista una supervisión humana para las decisiones más relevantes, el proceso sería más explicable, sobre todo si esta supervisión se exige ante las decisiones más críticas.

3. 3. DIFUSIÓN DE LA RESPONSABILIDAD

El desarrollo y uso de IA involucra múltiples actores: diseñadores, desarrolladores de software, fabricantes de hardware, operadores, usuarios... Esto provoca una difusión de la responsabilidad entre las distintas partes, complicando la identificación de quién debe responder en caso de que se cause un daño⁶⁴.

Como señala Wagner (2018, pp. 9-10), también es importante considerar la dispersión del control resultante del desacoplamiento de las actividades. Un producto o hardware puede soportar diferentes programas de distintos programadores que los usuarios pueden descargar y modificar a voluntad. Se puede combinar el software original con otro e ir variándolo hasta que quede prácticamente en una combinación única, como ocurre con muchos de nuestros teléfonos móviles. También se pueden juntar varias piezas de hardware u otros tipos de hardware, lo que hace que la tarea de atribuir responsabilidades sea muy complicada de acuerdo con los esquemas que tenemos hoy en día.

El desafío que esto representa es tan simple como: ¿quién debe ser responsable, el fabricante, el desarrollador del algoritmo, el proveedor del hardware, el usuario final que opera el sistema...? La falta de claridad en este punto puede complicar mucho las demandas de RC.

⁶⁴ Como señalan Benhamou y Ferland «*The number of stakeholders involved in the creation and operation of AI systems is concurrently rising: hardware manufacturers, software designers, sellers, equipment and software installers, facility owners, AI owners, AI users and trusted third parties, amongst others, may all have a role to play in ensuring that AI does not cause harm, and allocating liability in this context is not an easy task*», Benhamou y Ferland, 2021, pp. 168-170.

El principio de rendición de cuentas puede verse afectado si no hay claridad en este asunto, pues recordemos que «Este requisito exige establecer mecanismos que permitan garantizar la responsabilidad y rendición de cuentas sobre los sistemas de IA y sus resultados, tanto antes de su implantación como después de esta»⁶⁵.

Las posibles respuestas ante este desafío pueden ser variadas:

1. **Responsabilidad compartida en función del rol y control.** Como señala el documento de la OECD (2019, p. 9): «*AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of the art*».

Así se podría distribuir la responsabilidad entre los diversos actores en función del grado de control⁶⁶ y los diversos roles que cada uno tiene, de tal forma que habría una responsabilidad compartida⁶⁷. Sin pretender ser exhaustivo, podrían existir distintas responsabilidades:

- **Desarrollador del algoritmo:** sería responsable en la medida en que hubiera fallos en el diseño del algoritmo o se hubieran ignorado medidas de precaución razonables para evitar sesgos, errores o inseguridades. Este enfoque se basa en el principio de precaución y responsabilidad. Además los desarrolladores serían unos de los principales responsables de la robustez y seguridad técnica de la IA que también aparece en diversos documentos.

⁶⁵ Grupo Independiente de Expertos, 2019, *Directrices éticas*, 87, p. 22.

⁶⁶ Conviene recordar el Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza: «La Comisión considera que, en un futuro marco regulador, cada obligación debe dirigirse a la(s) persona(s) que esté(n) en mejor posición para abordar todo posible riesgo. Por ejemplo, mientras que los desarrolladores de IA pueden ser los que estén en mejor posición para abordar los riesgos derivados de la fase de desarrollo, su capacidad de controlar los riesgos durante la fase de uso puede ser más limitada. En este caso, el implementador debe ser objeto de la obligación correspondiente. Ello debe entenderse sin perjuicio de determinar qué parte debe ser responsable de los daños causados, a efectos de la responsabilidad civil ante los usuarios finales u otras partes que sufran daños, y de ofrecer un acceso efectivo a la justicia. Con arreglo a la legislación de la UE sobre responsabilidad con relación a los productos, la responsabilidad civil por los productos defectuosos se atribuye al productor, sin perjuicio de la legislación nacional, que también puede contemplar una indemnización a cargo de otras partes», Comisión Europea, 2020, *Libro blanco*, p. 27.

⁶⁷ En un artículo con un título muy descriptivo sobre la autonomía de la IA (*Machines without principals: Liability rules and artificial intelligence*) Vladeck proponía que, especialmente en casos donde las máquinas actúan de manera impredecible o cometen errores que no pueden ser atribuidos a fallos de diseño o fabricación, se estableciera una responsabilidad objetiva colectiva bajo la doctrina de la «*common enterprise*» («*each entity within a set of interrelated companies may be held jointly and severally liable for the actions of other entities that are part of the group*»). Se trataría de una RC cuyo fundamento último sería simplemente «*to protect a blameless party (the person who sustained injured) by making others bear the cost*», Vladeck, 2014, pp. 149 y ss.

- **Proveedor del hardware:** sería responsable si el fallo se originase en el hardware o si el hardware no fuera adecuado para las especificaciones del software o sistema de IA. Aquí se podría aplicar la RC objetiva para los defectos de fabricación, en línea con los principios de seguridad y robustez.
 - **Fabricante:** la RC del fabricante se encuentra recogida en la Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos, incluyendo en su ámbito objetivos los productos que incorporan sistemas de IA. Se trata de una RC objetiva ampliamente aceptada por la doctrina, la industria y los consumidores.
 - **Operador/usuario final:** si el usuario final operara el sistema de IA de manera negligente o incorrecta, por ejemplo, ignorando advertencias de seguridad o utilizando el sistema en un entorno no adecuado, debería asumir la responsabilidad. Los principios de transparencia y explicabilidad exigen que los usuarios sean conscientes de cómo operar y controlar la IA.
2. Podría pensarse en establecer un **sistema mixto de RC objetiva combinado con elementos subjetivos**. En la misma línea de lo anterior, se podría establecer una RC objetiva de todos los actores involucrados en el sistema de IA, de tal forma que la víctima fuera compensada de los daños y al mismo tiempo tomar en consideración la existencia de negligencia si se probase, para penalizar a los culpables. Esta matización subjetiva podría afectar, por ejemplo, al usuario final de la IA que haya sido negligente. Véase lo que se dice en el Principio 9 de la Declaración de Montreal: «5. *When damage or harm has been inflicted by an AIS, and the AIS is proven to be reliable and to have been used as intended, it is not reasonable to place blame on the people involved in its development or use*» (IVADO, 2018). A contrario, si se puede probar la negligencia del usuario final, lo lógico sería hacer responsable a este último.
 3. **Fondo de compensación para víctimas de IA.** En aquellos casos en que sea imposible identificar a un responsable directo o cuando exista un daño difuso que afecte a múltiples personas de manera simultánea, podría crearse un fondo de compensación⁶⁸. Este fondo sería financiado por las empresas que desarrollan, venden o implementan sistemas de IA y garantizaría que las víctimas recibieran compensación, independientemente de las dificultades para probar la culpa o negligencia.

⁶⁸ Por ejemplo, con ciertos matices, para el ámbito de los productos defectuosos propone un seguro obligatorio y un fondo de compensación García Teruel, 2021, 68, 2.4.

En la UE se está planteando esta posibilidad desde las primeras reflexiones⁶⁹ y lo volvieron a dejar abierto el grupo de expertos de alto nivel en su segundo entregable⁷⁰. Esto sería conforme con diversos principios como los de compensación y equidad, pues evitarían abandonar a su suerte a las víctimas cuando no fuera posible identificar al responsable directo.

4. **Cláusulas contractuales de responsabilidad entre actores.** En los contratos entre los diversos actores involucrados en el ciclo de vida de los sistemas de IA sería aconsejable establecer cláusulas contractuales que concretaran los diversos roles y las responsabilidades de cada uno, lo que ayudaría a fijar una RC más adecuada, proporcionada y justa.

Igualmente, los contratos de uso de IA también deberían incluir disposiciones que aclararan las responsabilidades en caso de mal uso por parte del usuario o de fallos en la configuración o integración del sistema.

3.4. AUTONOMÍA DE LA IA Y RESPONSABILIDAD HUMANA

La característica que diferencia la IA de cualquier tecnología precedente es la habilidad de la IA para actuar autónomamente⁷¹. A medida que la IA se vuelve más autónoma, surgen preguntas sobre hasta qué punto los humanos pueden o deben ser responsables de las decisiones que toman estos sistemas, especialmente si la IA actúa de manera impredecible o fuera del control de sus operadores⁷². Si bien los principios éticos subrayan que la **responsabilidad final siempre recae en los seres humanos**⁷³, es posible que los operadores

⁶⁹ Decían por ejemplo las Normas de Derecho civil sobre robótica: «Considera que, tal como sucede con el seguro de vehículos de motor, dicho sistema podría completarse con un fondo que garantizara la reparación de daños en los casos de ausencia de una cobertura de seguro; pide al sector de los seguros que desarrolle nuevos productos y tipos de ofertas adaptados a los progresos de la robótica», Parlamento Europeo, 2017, *Normas de Derecho civil*, 58.

⁷⁰ «Finally, civil liability rules must be able to ensure adequate compensation in case of harm and/or rights violations (either through strict or tort liability), and may need to be complemented with mandatory insurance provisions», Grupo Independiente de Expertos, 2019, *Policy and investment recommendations*, 27.2.

⁷¹ Scherer, 2016, p. 364.

⁷² Las Normas de Derecho civil sobre robótica consideraban que «en el supuesto de que un robot pueda tomar decisiones autónomas, las normas tradicionales no bastarán para generar responsabilidad jurídica por los daños ocasionados por el robot, ya que no permitirán determinar la parte que ha de hacerse cargo de la indemnización, ni exigir a dicha parte que repare el daño ocasionado», Parlamento Europeo, 2017, *Normas de Derecho civil*, AF.

⁷³ Esto ocurre habitualmente en Derecho. Por ejemplo Magrani recuerda que el art. 12 de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales supone que una persona es responsable en última instancia de la acción generada por una máquina, cuando establece: «Article 12. Use of automated message systems for contract formation. A contract formed by the interaction of an automated message system and a natural person, or by the

o diseñadores no puedan prever todas las acciones de la IA, lo que genera incertidumbre en cuanto a la RC⁷⁴.

La RC clásica comienza a resentirse cuando nos enfrentamos a sistemas complejos (compuestos por elementos diversos) en los que los cursos causales son difíciles de determinar y es difícil averiguar cuáles han sido las causas reales de los daños. En la IA, no se trata solo de complejidad, sino también de elementos interconectados y dependencia de datos externos, que le dan autonomía al sistema⁷⁵. La complejidad engloba todo el entorno en el que un sistema interactúa con otros dispositivos, productos, servicios, etc., configurando un ecosistema complejo donde el ecosistema puede llegar a ser tan inmenso como todo Internet.

Además, el riesgo de un producto puede surgir de la conectividad del producto, como: una pulsera inteligente para niños que permite rastrear y contactar con el niño (notificación RAPEX islandesa publicada en el sitio web de EU Safety Gate (A12/0157/19) o un vehículo cuyo software presenta fallos de seguridad de tal manera que permite que un tercero no autorizado acceda al sistema de control (notificación RAPEX alemana publicada en el sitio web de EU Safety Gate (A12/1671/15)).

Las respuestas a esta cuestión también pueden hacerse a través de otras ya vistas en los apartados anteriores:

1. **RC objetiva, especialmente en los sistemas de IA altamente autónomos.** La RC objetiva parece más aconsejable en los casos de sistemas de IA autónomos, en los que quizás no es fácil descubrir una negligencia más allá de una genérica culpa al poner en funcionamiento una IA autónoma y por ello impredecible en algunos supuestos.
2. **Fondos de compensación.** Por la misma razón anterior, en estos casos de sistemas de IA altamente autónomos parece más aconsejable la creación de fondos de compensación para las víctimas de la IA.
3. **Certificación y auditoría de los sistemas de IA altamente autónomos.** Como quiera que la autonomía se acompaña de impredecibilidad, resultaría especialmente importante que este tipo de sistemas cons-

interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract», Magrani, 2019, p. 6.

⁷⁴ Por ejemplo, los algoritmos con capacidad de aprender desafían la responsabilidad del fabricante o del diseñador, máxime cuando hay un *machine learning*, Mittelstadt et al., 2016, 11.

⁷⁵ La complejidad de los sistemas de IA es mucho mayor que cualquier producto que hayamos tenido antes. La IA, el IoT y la robótica se caracterizan por combinar «la conectividad, la autonomía y la dependencia de datos para llevar a cabo tareas con poco o ningún control o supervisión humanos», Comisión Europea, 2020, *Informe sobre las repercusiones*, 2.

tase con procedimientos de certificación y auditoría que evaluaran la seguridad de su uso cuando van a adoptar decisiones autónomas, lo que estaría basado en los principios de seguridad, transparencia y explicabilidad.

4. **Reforzar la supervisión humana.** En los sistemas de IA con alta autonomía debería haber un deber de supervisión constante, de tal manera que los operadores pudieran monitorizar el comportamiento de la IA y detectar los riesgos o fallos para evitar que se produjeran daños. Este deber reforzado de supervisión humana tendría que ir acompañado de la posibilidad de intervención manual por parte de las personas que lo están monitorizando y todo ello supondría un deber de diligencia que serviría, en su caso, para apreciar la negligencia si fallara.
5. La **Responsabilidad compartida** también podría servir en estos casos para saber quiénes son los actores responsables cuando la IA actúa con mayor autonomía, lo que sería una exigencia de la transparencia y la explicabilidad.

3. 5. DAÑOS COLECTIVOS Y DIFUSOS

En los daños que puede causar la IA se pueden intensificar algunas categorías de daños, ya existentes y conocidos por el Derecho, pero que conviene tener en cuenta.

Por ejemplo, conviene recordar esquemáticamente el concepto de **intereses difusos** que estarían entre los intereses individuales y los colectivos. Interés individual es aquél que afecta y pertenece a un individuo de tal manera que su lesión puede dar lugar a RC. Por otro lado un interés colectivo se refiere a aquello cuya titularidad corresponde al colectivo y las medidas de reparación, si existen, serán exigibles por quien tenga representación del interés colectivo. Los intereses difusos se encuentran en un terreno intermedio por ser una lesión de algo individual que se causa a una colectividad. Pero una cosa son lesiones individuales hechas a un colectivo, lo que se puede solucionar a través de las acciones colectivas y otra aquellos casos en los que no llega a producirse una lesión individual que legitime una acción de RC, pero esa molestia se produce a un colectivo. Un sesgo algorítmico que genera una discriminación en sectores como el crédito, la sanidad o el empleo puede ocasionar una lesión individual a un colectivo de personas, cuando se les produce un daño concreto que pueden reclamar por RC y a la vez una lesión de intereses difusos de todas aquellas personas que *podrían* haber sufrido el daño, porque han sido discriminadas aunque no hayan llegado a recibir el daño.

En la discriminación a gran escala a través de decisiones algorítmicas o en las decisiones automatizadas que afectan a miles de personas se pueden producir daños a colectivos y lesiones de intereses difusos. En los supuestos de daños individuales que afectan a un colectivo de personas, la solución tendrá que ver con el régimen de **acciones colectivas** que ya existe, con mayor o menor acierto, en la UE.

En los supuestos de lesiones a intereses difusos se pueden estar poniendo en cuestión principios como los de Bienestar, Equidad, Diversidad e Inclusión.

Diversas actuaciones que se podrían tener en cuenta son:

1. **Establecimiento de criterios para cuantificar daños difusos.** Sería adecuado desarrollar criterios que permitieran cuantificar los daños difusos y graduales causados por la IA en contextos en los que el daño afectara a un grupo o colectividad. Estos criterios podrían basarse en la magnitud del impacto y en la repetición del daño, midiendo los efectos acumulativos de las decisiones de la IA. Tales criterios servirían para medir si se cumplen principios como: «*AI must be designed and trained so as not to create, reinforce, or reproduce discrimination based on -among other things- social, sexual, ethnic, cultural, or religious differences*»⁷⁶.
2. **Auditoría algorítmica para identificar daños difusos.** Dentro de los sistemas de auditoría propuestos en otros apartados, podrían establecerse auditorías algorítmicas que pudieran identificar patrones de discriminación o perjuicio causados por la IA⁷⁷. Además de los principios de bienestar y equidad, esto favorecería los de transparencia y explicabilidad⁷⁸.
3. En los **fondos de compensación** vistos en otros apartados, podría verse si podrían incluirse soluciones para los daños colectivos e incluso formas de compensación para las lesiones a los intereses difusos.

⁷⁶ IVADO, 2018, Principio 6 Equidad.

⁷⁷ Por ejemplo, Floridi et al. en su recomendación 4 proponen: «*Develop auditing mechanisms for AI systems to identify unwanted consequences, such as unfair bias, and (for instance, in cooperation with the insurance sector) a solidarity mechanism to deal with severe risks in AI-intensive sectors*», Floridi et al., 2018, p. 702.

⁷⁸ El principio de transparencia algorítmica «exige la visibilidad, la cognoscibilidad, la auditabilidad y la explicabilidad de los factores intervinientes en las decisiones tomadas con algoritmos a las personas que utilizan, regulan, y son afectadas por los sistemas de IA que emplean dichos algoritmos», Llano Alonso, 2024, p. 194.

3. 6. DAÑOS FUTUROS E INCIERTOS

El principio de precaución subraya la necesidad de anticipar y evitar posibles riesgos futuros de la IA. Sin embargo, la incertidumbre inherente al desarrollo tecnológico hace difícil prever todos los efectos negativos, lo que complica la prevención y la responsabilidad por daños potenciales que aún no se han manifestado.

Es importante recordar que el concepto de daño es dinámico y ha variado a lo largo del tiempo, por lo que aplicamos, por ejemplo, nuestros Códigos Civiles a realidades que ni siquiera se podían haber soñado cuando se promulgaron los Códigos. Una de las grandes incertidumbres con las que tenemos que convivir es la necesidad de conocer los riesgos de la IA. Por ejemplo, no conocemos los riesgos para la salud mental de los usuarios que pueden generar las aplicaciones de IA que implican la colaboración con robots o sistemas de IA humanoides en el hogar o en entornos laborales⁷⁹: es concebible que realidades que hoy no conocemos se consideren daños en el futuro. También puede haber daños importantes que no seamos capaces de prever⁸⁰.

Lo anterior está relacionado con principios como el de prevención del daño o seguridad. Algunas ideas que se podrían explorar son:

1. Establecimiento de **mecanismos de monitoreo y evaluación a largo plazo** para los sistemas de IA⁸¹. Esto implicaría una supervisión continua de los efectos de la IA, incluso años después de su implementación, para detectar daños potenciales antes de que se manifesten completamente y evitar que las víctimas se vean afectadas sin protección.
2. **Revisión y actualización de las regulaciones.** Los tiempos de los legisladores deberían acomodarse a los tiempos de las realidades cambiantes. Baste recordar lo que ha costado en la UE la elaboración de la Ley de Inteligencia Artificial y cómo, durante su tramitación, surgieron novedosas aplicaciones como la IA generativa que no esta-

⁷⁹ Comisión Europea, 2020, *Report on the*, p. 9.

⁸⁰ Dentro de los asuntos a largo plazo el Principio 21 de Asilomar señala «*Risks: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact*» Future of Life Institute, 2017.

⁸¹ Por ejemplo las Recomendaciones de la UNESCO señalan: «Los Estados Miembros deberían alentar y promover la investigación colaborativa sobre los efectos de la interacción a largo plazo de las personas con los sistemas de IA, prestando especial atención a las consecuencias psicológicas y cognitivas que estos sistemas pueden tener en los niños y los jóvenes. Para ello deberían utilizarse múltiples normas, principios, protocolos, enfoques disciplinarios y un análisis de la modificación de las conductas y los hábitos, así como una cuidadosa evaluación de los impactos culturales y sociales posteriores», UNESCO, 2022, 129.

ba inicialmente contemplada en la Ley. Teniendo en cuenta los avances en estas materias, procedimientos legislativos que tardan años en culminar pueden nacer obsoletos⁸². Las propias Directrices señalan que la normativa, como método no técnico, debe someterse a evaluación constante⁸³.

Deberíamos tender hacia una regulación proactiva⁸⁴ y no simplemente reactiva con años de retraso.

Además, como señalaba el Principio 3 de Asilomar: «3) *Science-Policy Link: There should be constructive and healthy exchange between AI researchers and policy-makers*» (Future of Life Institute, 2017).

3. Diseño de **fondos de compensación** podrían estar diseñados para poder hacer frente a contingencias futuras que quizás todavía no se puedan prever.

4. BIBLIOGRAFÍA UTILIZADA

- Abbott, R. B. (2018). The reasonable computer: Disrupting the paradigm of tort liability. *George Washington Law Review*, 86 (1), 1-68.
- Atienza Navarro, M. L. (2023). ¿Son necesarias reglas especiales para los daños causados por inteligencia artificial? En *Derecho e Inteligencia Artificial [El jurista ante los retos de la era digital]*. Thomson Reuters Aranzadi.
- Benhamou, Y., y Ferland, J. (2021). Artificial intelligence & damages: Assessing liability and calculating the damages. En *Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (pp. 168-170). Thomson Reuters.
- Borghetti, J.-S. (2019). Civil liability for artificial intelligence: What should its basis be? *La Revue des Juristes de Sciences Po*, (17), 1-30.
- Bostrom, N., y Yudkowsky, E. (2014). The ethics of artificial intelligence. En K. Frankish & W. Ramsey (Eds.), *The Cambridge handbook of artificial intelligence* (pp. 316-334). Cambridge University Press.

⁸² Los diferentes tiempos del legislador y de los avances tecnológicos son un problema en materia de IA y de no fácil solución, porque la legislación necesita reflexión y debate. «*Even though the “legal lag” is more complex than it may seem, the speed of change, in particular, is still repeatedly a difficult challenge in relation to the inertia of traditional regulation. Legislative processes aimed at learning technologies with increasing agency require reflection, critical studies, and more knowledge in order to be able to find the desirable societal balances between various interests*», Larsson, 2020, p. 447.

⁸³ Grupo Independiente de Expertos, 2019, *Directrices éticas*, 103.

⁸⁴ «*Proactive measures and strict regulations are needed to ensure that AI development follows ethical guidelines and remains aligned with human values to prevent harmful outcomes*», (Bostrom y Yudkowsky, 2014)

- Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, 107(1), 1-68. <https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1>
- Colmenarejo, A. B., Nannini, L., Rieger, A., Scott, K. M., Zhao, X., Patro, G. K., Kasneci, G., & Kinder-Kurlanda, K. (2022). Fairness in agreement with European values: An interdisciplinary perspective on AI regulation. En *AIES 2022 - Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 107-118). Association for Computing Machinery. <https://doi.org/10.1145/3514094.3534158>
- Comisión Europea. (2020). *Libro blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza*. COM(2020) 65 final. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065>
- Comisión Europea. (2019). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Generar confianza en la inteligencia artificial centrada en el ser humano*. COM(2019) 168 final. <https://eur-lex.europa.eu/legal-content/ES/TXT/DOC/?uri=CELEX:52019DC0168>
- Comisión Europea. (2020) Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica. COM/2020/64 final. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0064>
- Comisión Europea, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, Brussels, 19.2.2020 COM(2020) 64 final, p. 9. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0064>
- Dignum, V. (2018). Ethics in artificial intelligence: Introduction to the special issue. *Ethics and Information Technology*, 20(1), 1-3. <https://doi.org/10.1007/s10676-018-9450-z>
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., y Vayena, E. (2018). AI4People: An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
- García Teruel, R. M. (2021). El derecho de daños ante la inteligencia artificial y el machine learning: Una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea. En F. Roca Guillamón (Ed.), *Cuestiones clásicas y actuales del derecho de daños*. Aranzadi.
- Hagendorff, T. (2020). The ethics of AI ethics: An evaluation of guidelines. *Minds and Machines*, 30(1), 99-120. <https://doi.org/10.1007/s11023-020-09517-8>
- Future Of Life Institute. (2017). Asilomar AI principles. <https://futureoflife.org/ai-principles/>
- Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial. (2019). *Directrices éticas para una IA fiable*. Comisión Europea. <https://doi.org/10.2759/177365>

- Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial. (2019). *Policy and investment recommendations for trustworthy AI*. Comisión Europea. <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>
- IEEE. (2019). *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (1ª ed.). <https://ethicsinaction.ieee.org/>
- Institut de Valorisation des Données (IVADO). (2018). *Montreal declaration for a responsible development of artificial intelligence*. <https://www.montrealdeclaration-responsibleai.com/>
- IPSOS. (2023). *Global views on AI 2023*. IPSOS. <https://www.ipsos.com/sites/default/files/ct/news/documents/2023-07/Ipsos%20Global%20AI%202023%20Report.pdf>
- Larsson, S. (2020). On the governance of artificial intelligence through ethics guidelines. *Asian Journal of Law and Society*, 7(3), 437-451. <https://doi.org/10.1017/als.2020.19>
- Llano Alonso, F. H. (2024). Ética(s) de la inteligencia artificial y derecho: Consideraciones a propósito de los límites y la contención del desarrollo tecnológico. *Derechos y Libertades*, 51, 177-199. <https://doi.org/10.20318/dyl.2024.8587>
- Magrani, E. (2019). New perspectives on ethics and the laws of artificial intelligence. *Internet Policy Review*, 8(3). <https://doi.org/10.14763/2019.3.1420>
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., y Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21. <https://doi.org/10.1177/2053951716679679>
- Müller, L. (2022). Domesticating artificial intelligence. *Moral Philosophy and Politics*, 9(2), 219-237. <https://doi.org/10.1515/mopp-2020-0054>
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- OdiseIA, PwC, Google, Microsoft, IBM, y Telefónica. (2022). *Guía de buenas prácticas en el uso de la inteligencia artificial ética*. Recuperado de <https://www.digitalidades.org/guia-de-buenas-practicas-en-el-uso-de-la-inteligencia-artificial-etica/>
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
- Oxford Internet Institute. (2020). *Global attitudes towards AI, machine learning & automated decision making*. University of Oxford. <https://www.oii.ox.ac.uk/research/global-attitudes-ai-2020.pdf>
- Parlamento Europeo. (2022). *Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI))*.
- Parlamento Europeo. (2017). *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de derecho civil sobre ro-*

- bótica* (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
- Parlamento Europeo. (2020). *Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL)).
- Parlamento Europeo, Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html#title2
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA). COM/2022/496 final <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>
- Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. COM/2022/495 final <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0495>
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>
- Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353-400. <http://dx.doi.org/10.2139/ssrn.2609777>
- Selbst, A. D. (2020). Negligence and AI's human users. *Boston University Law Review*, 100, 1315-1376.
- Stamboliev, E., y Christiaens, T. (2024). How empty is trustworthy AI? A discourse analysis of the ethics guidelines of trustworthy AI. *Critical Policy Studies*. <https://doi.org/10.1080/19460171.2024.2315431>
- Susskind, R. (2019). *Online courts and the future of justice*. Oxford University Press.
- UNESCO. (2022). *Recomendación sobre la ética de la inteligencia artificial*. https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa
- Van Wynsberghe, A. (2016). *Healthcare robots: Ethics, design and implementation*. Routledge.
- Velasco Perdigones, J. C. (2021). Fundamentos para la atribución de responsabilidad civil extracontractual en la “era tecnológica”. En J. Cruz Ángeles, M. Novo Foncubierta, B. Martín Novo, y M. Paniagua Zurera (Coords.), *El sistema jurídico ante la digitalización. Estudios de derecho privado*. Tirant lo Blanch.

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, 89(1), 117-150. <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/6>

Wagner, G. (2018). Robot liability. *SSRN*. <http://dx.doi.org/10.2139/ssrn.3198764>

Los sistemas de inteligencia artificial, ¿productos defectuosos?

MANUEL ORTIZ FERNÁNDEZ

*Profesor Ayudante Doctor de Derecho Civil
Universidad Miguel Hernández de Elche*

Sumario: 1. CUESTIONES PRELIMINARES. 2. LA LEY DE INTELIGENCIA ARTIFICIAL. 2.1. Concepto y características básicas de la inteligencia artificial. 2.2. El riesgo y la intervención humana: las actividades prohibidas y la clasificación de los sistemas. 3. LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE SISTEMAS INTELIGENTES. 3.1. Las relaciones entre las dos propuestas de Directiva. 3.2. La responsabilidad civil en la (revisada) Directiva sobre productos defectuosos. 3.2.1. Reflexiones acerca del concepto de producto defectuoso y los sujetos responsables. 3.2.2. Régimen de responsabilidad civil y presunciones. 3.3. La propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial. BIBLIOGRAFÍA.

1. CUESTIONES PRELIMINARES

Para comenzar, por más obvio que parezca, hemos de señalar que la incorporación de la inteligencia artificial comporta innegables aspectos positivos, pero también importantes retos¹. Su naturaleza *sui generis*, su compleji-

¹ Sobre su repercusión en el ámbito jurídico, *vid.* el Informe Innovación & Tendencias del Sector Legal 2024, Aranzadi, La Ley, marzo 2024. Disponible en: <https://goo.su/nWFz1Ur> (fecha de última consulta: 01.07.2024). Asimismo, encontramos las recientes recomendaciones emitidas por el Grupo de Trabajo sobre Justicia Digital e Inteligencia Artificial de la Comisión Europea para la eficiencia de la justicia sobre el uso de la inteligencia artificial generativa en el trabajo jurídico (12 de febrero de 2024), con las que se pretende presentar una visión preliminar sobre lo que los jueces

dad y la imposibilidad para conocer, *a priori*, la actuación de la máquina, han provocado que se plantee la necesidad de aprobar una normativa específica. Y es que, las reglas tradicionales no se adaptan adecuadamente a esta nueva realidad. Piénsese, por ejemplo, en la responsabilidad por hecho ajeno y la atribución de culpa.

En este sentido, la estrategia europea parte de tres bloques de actuaciones. De un lado, aparecen las denominadas normas horizontales sobre los sistemas de inteligencia artificial, cuyo máximo exponente se identifica con el Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021 (en adelante, Ley de Inteligencia Artificial²). Esta última, a través de los requisitos, condiciones, exigencias y, en particular, a partir de la clasificación de los sistemas³, incorpora una suerte de principios que tratan de evitar (o, al menos, reducir), los daños producidos como consecuencia del uso de esta tecnología⁴.

y otros profesionales del sector público de la justicia pueden esperar del uso de herramientas de inteligencia artificial generativa en su trabajo. Más información en: <https://rm.coe.in/cepej-gt-cyberjust-2023-5final-en-note-on-generative-ai/1680ae8e01> (fecha última consulta: 20.05.2024). A este respecto, un ejemplo de mal uso de la inteligencia artificial en este sector puede detectarse en la condena impuesta por un tribunal federal norteamericano que ha suspendido de ejercicio un abogado por presentar un escrito procesal elaborado por inteligencia artificial que incluía precedentes inexistentes. Para más información, *vid.*: <https://goo.su/AszzOB> (fecha última consulta: 20.05.2024).

² Aprobado por el Parlamento Europeo el 13 de marzo de 2024 y ratificado definitivamente por el Consejo el 21 de mayo.

³ Se entiende que estamos ante un sistema de alto riesgo cuando:

- Con independencia de que un sistema de IA se comercialice o se ponga en servicio independientemente de los productos contemplados en las letras a) y b), dicho sistema de IA se considerará de alto riesgo cuando se cumplan las dos condiciones siguientes: (a) el sistema de IA está destinado a utilizarse como componente de seguridad de un producto, o el sistema de IA es en sí mismo un producto, cubierto por la legislación de armonización de la Unión enumerada en el anexo II; (b) el producto cuyo componente de seguridad con arreglo a la letra a) es el sistema de IA, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad por terceros, con vistas a la comercialización o puesta en servicio de dicho producto con arreglo a la legislación de armonización de la Unión enumerada en el anexo II.

- Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA a que se refiere el anexo III.

⁴ Sobre el particular, cabe aludir al Convenio internacional sobre Inteligencia Artificial, elaborado por el Comité sobre Inteligencia Artificial del Consejo de Europa (y aprobado por esta institución el día 14 de marzo de 2024) que pretende establecer un conjunto de principios, normas y derechos destinados a garantizar que el diseño, el desarrollo y la puesta en servicio de sistemas de inteligencia artificial sean plenamente compatibles con el respeto de los derechos humanos, el funcionamiento de la democracia y la del Estado de Derecho. Asimismo, contempla una serie de medidas para garantizar que las víctimas reciban una adecuada indemnización por los daños causados por estos sistemas. Para más información, *vid.*: <https://rm.coe.int/brochure-artificial-intelligence-es-march-2023-print/1680aab8e8> (fecha de última consulta: 01.07.2024). A este respecto, hay que reseñar la Decisión (UE) 2022/2349 del Consejo, de 21 de noviembre de 2022, por la que se autoriza la apertura de negociaciones en nombre de la Unión Europea con vistas a un convenio del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho.

Asimismo, incorpora determinadas prohibiciones para ciertas prácticas de inteligencia artificial; una serie de requisitos para los sistemas de inteligencia artificial de alto riesgo; reglas de transparencia para los sistemas destinados a interactuar con personas físicas, sistemas de reconocimiento de emociones y sistemas de categorización biométrica, y sistemas de inteligencia artificial utilizados para generar o manipular contenido de imagen, audio o vídeo; normas sobre seguimiento y vigilancia del mercado.

De otro lado, disponemos de las normas sobre seguridad de los productos⁵, entre las que existe una legislación general (la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos) y una normativa sectorial o especial (entre otras, la Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (refundición) o la Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes).

Por otro lado, podemos mencionar el proyecto de Ley de atención a la clientela y comentario sobre el uso de la inteligencia artificial, aprobado el 27 de febrero de 2024 por el Consejo de Ministros y remitido al Congreso de los Diputados para comenzar su tramitación parlamentaria por segunda vez (pues en 2022 se había presentado otro proyecto de Ley, que caducó). La finalidad última es que la clientela reciba «una atención de calidad, personalizada y accesible» cuando solicita información o presentan reclamaciones ante empresas que entra dentro del ámbito de aplicación de la Ley.

⁵ Podemos indicar que, para modernizar y adaptar la regulación al entorno digital, existen diversas propuestas (unas aprobadas y otras en trámites de aprobación) en este campo. *Vid.*, entre otras:

- El Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

- El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

- La propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para productos con elementos digitales («Cyber Resilience Act»), de 2022. Cabe destacar que recientemente se ha emitido la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2024, sobre la propuesta de reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020 (12 marzo 2024).

- La Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a las máquinas y sus partes y accesorios, de 2021.

- La Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 2021.

Por último, tenemos las normas sobre responsabilidad civil para lo cual, en abstracto, aparecían tres opciones: utilizar las normas vigentes, reformar el régimen jurídico o aprobar otras disposiciones legales (ya fuera a modo directo, a través de un reglamento, ya con una directiva). Sobre el particular, a pesar de iniciativas anteriores, se ha optado por una vía intermedia; a saber, revisar la Directiva del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos y aprobar una nueva Directiva del Parlamento Europeo y del Consejo, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (propuesta de Directiva sobre responsabilidad en materia de IA). En realidad, no se solapan entre ellas, sino que actúan en ámbitos diferentes para ofrecer una normativa completa y armonizada en toda la Unión Europea.

Además, estas últimas se complementan con otras disposiciones que están vigentes y que cubren un espacio diferente de actuación. A este respecto, las legislaciones nacionales permiten interponer reclamaciones contra una gama más amplia de personas responsables y contemplan una categoría más extensa de daños indemnizables que, a menudo, incluye también los servicios (no solo los productos). A ello, hay que anudar otras normas europeas con ámbitos especiales de aplicación como la Directiva (UE) 2019/771 o la Directiva (UE) 2019/770.

En todo caso, estas tres realidades no cabe interpretarlas como compartimentos estancos. Muy al contrario, se encuentran íntimamente ligadas. Así las cosas, las normas sobre seguridad de los productos, al igual que las normas horizontales, contribuyen a la reducción del riesgo de producción de perjuicios, aunque no lo eliminan por completo. De hecho, la Ley de Inteligencia Artificial incluye disposiciones sobre seguridad y conformidad directamente aplicables a la inteligencia artificial. En todo caso, cuando estemos ante un sector que cuente con una norma especial (como ocurre, por ejemplo, en el sanitario con el Reglamento (UE) 2017/745), la Ley de Inteligencia Artificial queda relegada a la subsidiariedad y supletoriedad, como se deduce del aforismo *lex specialis derogat generalis*.

Igualmente, las primeras (las disposiciones sobre seguridad) se presentan como un complemento de las normas sobre responsabilidad civil (como «dos caras» de la misma moneda), pues a pesar de que no resuelven los problemas relacionados con la responsabilidad, son muy relevantes para determinar la misma por cuanto se tienen en cuenta para declarar su existencia. En otras palabras, ambas actúan en situaciones distintas y se refuerzan mutua y necesariamente. Igualmente, las disposiciones especiales que se encarguen del tema

relativo al Derecho de daños han de tener en cuenta la «norma horizontal» para, partiendo de las premisas que esta última incluye, articular un sistema de responsabilidad civil acorde a los principios de la Unión Europea.

Como quiera que el funcionamiento del mercado precisa del constante intercambio de productos y servicios entre los países miembros (y con otros situados fuera de la Unión) y que esta actividad puede entrañar riesgos, la legislación debe actuar en dos momentos diferentes: con carácter *ex ante*, mediante normas sobre seguridad de los productos⁶, que supriman, reduzcan o minimicen los posibles daños causados; *ex post*, cuando el producto ha causado el perjuicio, para resarcir a la víctima.

En suma, la importancia de estas cuestiones puede detectarse en otras medidas adoptadas tales como el denominado Pacto de IA (que busca el compromiso voluntario de la industria de comenzar a aplicar los requisitos de la Ley de Inteligencia Artificial antes de que transcurra el plazo legal de su entrada en vigor), la iniciativa presentada por el Consejo de la Unión Europea, para reformar el Reglamento (UE) 2021/1173, por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea, a fin de que esta entidad pueda facilitar el acceso a sus recursos informáticos a las empresas emergentes y a la comunidad científica, para desarrollar aplicaciones de IA específicas o las Conclusiones sobre la capacitación digital para proteger y hacer cumplir los derechos fundamentales en la era digital (20 octubre 2023). Así como en relación con la propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a las patentes esenciales para normas (COM (2023) 232 final), de abril de 2023, una norma destinada a atraer a los innovadores a la UE y garantizar el acceso de los consumidores europeos a los productos basados en las tecnologías más avanzadas (sobre la cual el Parlamento Europeo adoptó su posición negociadora el 28 de febrero de 2024).

Y tienen repercusión, incluso, fuera de la Unión Europea⁷. Véase, a este respecto, la reciente creación del primer consorcio dedicado a la seguri-

⁶ Entre las normas sobre seguridad de los productos, existe una legislación general (la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos) y una normativa sectorial o especial (entre otras, la Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (refundición) o la Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes). Cabe indicar que, para modernizar y adaptar la regulación al entorno digital, existen diversas propuestas (unas aprobadas y otras en trámites de aprobación) en este campo.

⁷ También podemos destacar los debates mantenidos en la celebración de la quinta edición de la Mesa de Atenas sobre IA y estado de Derecho (The Athens Roundtable on AI and the Rule of Law). Así, se centraron en los esfuerzos nacionales para avanzar en la regulación vinculante, como los esfuerzos legislativos federales de EEUU los próximos pasos de las agencias federales basados en la Orden Ejecutiva 14110 de EEUU sobre el Desarrollo y Uso Seguro y Confiable de la Inteligencia

dad de la inteligencia artificial en Estados Unidos (Consortio del Instituto de Seguridad de IA (AI Safety Institute Consortium, AISIC). Se trata de un organismo dependiente del Instituto Nacional de Estándares y Tecnología (NIST) que reunirá a creadores y usuarios de IA, académicos, investigadores gubernamentales y de la industria, y organizaciones de la sociedad civil, en apoyo al desarrollo y despliegue de tecnologías de inteligencia artificial seguras y confiables. Igualmente, cabe destacar la política de gobernanza de inteligencia artificial aprobada por la Casa Blanca en desarrollo de la orden ejecutiva 14110 sobre el desarrollo y uso de una inteligencia artificial segura y confiable, emitida el pasado mes de octubre por el presidente Biden.

A este respecto, el Memorandum «Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence» (Fomento de la gobernanza, la innovación y la gestión de riesgos en el uso de la inteligencia artificial por parte de las agencias), elaborado por la oficina ejecutiva de gestión y presupuestos de la Casa Blanca, establece nuevos requisitos y orientaciones para la gobernanza, la innovación y la gestión de riesgos de los sistemas de IA utilizados o adquiridos por la Administración de los EEUU. O la aprobación (el 23 de julio de 2023), por parte de China, de las denominadas «Medidas Generativas de IA», que entraron en vigor el 15 de agosto de 2023. Se trata de una suerte de directrices provisionales para la actividad y gestión de la inteligencia artificial, como resultado de un esfuerzo conjunto de seis organismos gubernamentales, entre ellos la Administración de Ciberseguridad de China (CAC), la Comisión Nacional de Desarrollo y Reforma y el Ministerio de Ciencia y Tecnología.

Igualmente, en América Latina hay que aludir a Perú, que está liderando la regulación de la inteligencia artificial habiendo establecido un marco legal que busca equilibrar la innovación tecnológica con la protección de los derechos fundamentales de sus ciudadanos. De esta suerte, el 30 de abril de 2024

Artificial, la Ley de IA de la Unión Europea y la regulación de la IA generativa de China. Los diálogos también abarcaron los esfuerzos intergubernamentales, incluido el impacto del Proceso de IA de Hiroshima del G7 en la gobernanza empresarial, el alcance de la Recomendación de Ética de la IA de la UNESCO (y los subsiguientes esfuerzos de implementación), el potencial de una iniciativa de gobernanza mundial de la IA derivada del Órgano Consultivo de Alto Nivel de la ONU sobre IA, y el trabajo basado en pruebas del Observatorio de Políticas de IA de la OCDE.

Igualmente, se pueden mencionar las recomendaciones sobre el uso de la inteligencia artificial por parte de los profesionales, aprobadas por el grupo de trabajo sobre inteligencia artificial del Colegio de Abogados de Nueva York (NYSBA Task Force on Artificial Intelligence). Dicho informe se ocupa del impacto legal, social y ético de la Inteligencia Artificial y la Inteligencia Artificial generativa en el ejercicio profesional y se suma a los ya publicados por otras instituciones sobre el mismo tema, de los que podemos destacar los emitidos por el Colegio de Abogados de California; por la Task Force sobre Uso Responsable de la IA Generativa AI y sobre casos y políticas de uso de la IA generativa por abogados, del MIT Law y la Guía «A Supervisory AI Agent Approach to Responsible Use of GenAI in the Legal Profession» del Centro CodEX de la Stanford Law School.

se presentó el proyecto de Reglamento que acompaña a la Ley N.º 31814, la cual promueve el uso de la inteligencia artificial para el desarrollo económico y social del país⁸.

Asimismo, el pasado 21 de marzo de 2024, la Asamblea General de la ONU adoptó la resolución «Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible» (A/78/L.49), respaldada por más de 120 Estados miembros. En suma, trata de que los Estados se abstengan de utilizar sistemas de inteligencia artificial que no puedan funcionar de conformidad con las normas internacionales de derechos humanos o los pongan en riesgo. Por el contrario, plantea la necesidad de respeto, protección y promoción de los derechos humanos en el diseño, el desarrollo, el despliegue y el uso de esta tecnología.

Y es que, como se pone de relieve en el informe de la Oficina de Ciencia y Tecnología del Congreso de los Diputados («Oficina C»), «Avances en neurociencia: aplicaciones e implicaciones éticas», desde 2012 la inversión en este ámbito se ha multiplicado por 21, sobrepasando los 30 mil millones de euros⁹.

2. LA LEY DE INTELIGENCIA ARTIFICIAL

2.1. CONCEPTO Y CARACTERÍSTICAS BÁSICAS DE LA INTELIGENCIA ARTIFICIAL

En primer lugar, conviene que, en primer lugar, establezcamos qué se viene entendiendo por sistema de inteligencia artificial¹⁰. Por un lado, debemos tener en cuenta que la premisa básica de esta tecnología es que las máquinas puedan simular procesos de inteligencia humana. Así, en 1950, Alan Turing propuso el denominado *Turing Test* para determinar si una máquina era inteli-

⁸ Sobre el particular, *vid* Tuset Varela, D. (2024). La regulación de la inteligencia artificial en Perú: liderando el desarrollo ético y responsable de la IA en América Latina. *Diario LA LEY*, (83), 1-13.

⁹ Para más información, *vid*. Sanz de Galdeano, M. (2024). Neuroderechos: Todavía en las afueras del Derecho (A propósito de la comparecencia de Rafael Yuste en el Congreso). *Diario LA LEY*, (81), 1-5.

¹⁰ Parte de la doctrina aboga por la utilización del término «toma de decisiones automatizada». En este sentido, *vid*. Kemp, R. (2018). Legal Aspects of Artificial Intelligence, 2. Disponible en: <http://www.kempitlaw.com/wp-content/uploads/2018/09/Legal-Aspects-of-AI-Kemp-IT-Law-v2.0-Sep-2018.pdf> (fecha de última consulta: 01.07.2024).

gente. En este sentido, se podría predicar tal rasgo de la misma si un humano no era capaz de diferenciarla de otra persona¹¹. Por otro lado, en 1955 se planteó la realización de un proyecto de investigación en el que se partía de que cada aspecto del aprendizaje o cualquier otra característica de la inteligencia podía describirse, en principio, con tanta precisión, que era posible crear una máquina para simularla¹². En suma, se trataba de que estos robots usaran el lenguaje, formaran abstracciones y conceptos y resolvieran problemas reservados para los seres humanos¹³.

Además, al aproximarnos a estas cuestiones, hemos de tener presente que la doctrina diferencia entre dos tipos de inteligencia artificial¹⁴. Sea como fuere, destaca el autor citado que esta distinción no tiene excesivo sentido, ya que se asienta sobre la «falacia de la inteligencia artificial», en la medida en que está basada en la creencia de que la única manera de desarrollar sistemas que lleven a cabo tareas al nivel de los expertos es replicar los procesos de pensamiento de los especialistas humanos.

A pesar de que las instituciones europeas han elaborado y propuesto diferentes definiciones, el concepto que vamos a seguir es el contemplado en la Ley de Inteligencia Artificial. Esta última que propone una única descripción para los sistemas de inteligencia artificial razonablemente amplia y que, además, puede adaptarse a los cambios que se sucedan en el futuro. En este sentido, el artículo 3.1 de la Ley de Inteligencia Artificial destaca que se trata de «un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como pre-

¹¹ Turing, A. (1950). Computing Machinery and Intelligence. *Mind*, 59(236), 433-460.

¹² En este sentido, McCarthy, J., et al. (1955). A proposal for the dartmouth summer research project on artificial intelligence. 1-13. Disponible en: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> (fecha de última consulta: 01.07.2024).

¹³ Como destaca Murphy, R.R. (2019). *Introduction to AI Robotics*. The MIT Press, pp. 3-4, la inteligencia artificial puede definirse como la ciencia dedicada a realizar que las máquinas actúen de forma inteligente. No obstante, el autor citado reconoce que se trata de un concepto controvertido. Para concluir cuando estamos ante un robot con inteligencia artificial pone especial énfasis en las aplicaciones que puede desarrollar, a saber, que sea capaz de aprender, planificar, razonar, resolver problemas, adquirir conocimiento a partir de la representación e incorporar visión por computador. En este sentido, cabe señalar que, como apunta la doctrina, el propio término de inteligencia es sumamente variable y depende de la perspectiva desde la que se observe. En igual sentido, *vid.* Zurita Martín, I. (2020). *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*. Reus, p. 12; Churnin, S. (2011). *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*. Servicio de Publicaciones de la Facultad de Derecho. Universidad Complutense de Madrid, p. 21.

¹⁴ A este respecto, *vid.* Solar Cayón, J.I. (2019). *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*. Aranzadi, pp. 23-25.

dicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales».

Como destaca la doctrina¹⁵, la última decisión «ha sido la de aproximar su definición a la propuesta por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), en un intento de facilitar posteriores negociaciones para la elaboración de un convenio internacional que dote a la IA de un marco jurídico global». Así las cosas, destacan los autores citados la necesidad de relacionar la definición con el considerando 12 de la Ley de Inteligencia Artificial, toda vez que es necesario, por un lado, diferenciar estos sistemas de los sistemas de software tradicionales más sencillos. Por otro lado, debido a que la Ley de Inteligencia Artificial no incluye a los sistemas que se basan en reglas definidas únicamente por personas físicas para ejecutar operaciones automáticamente.

Y, por último, porque se «resalta su capacidad de inferencia, que incluye la de derivar modelos y/o algoritmos a partir de entradas/datos; de funcionar con arreglo a objetivos explícitos o implícitos (que pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico); de funcionar con distintos niveles de autonomía (con independencia o sin intervención humana) y de mostrar una capacidad de adaptación o autoaprendizaje que le permite modificar su comportamiento durante su utilización».

Así, por ejemplo, algunos autores¹⁶ incluyen, como subcampos de la inteligencia artificial, el aprendizaje automático (*machine learning*), el aprendizaje profundo (*deep learning*), el procesamiento del lenguaje natural (*natural language processing*) y la visión por computador (*computer vision*). A partir de estas premisas, podemos destacar las siguientes características básicas de la inteligencia artificial:

— Influencia en entornos físicos o virtuales: robótica. Se conoce como *software* al conjunto de los componentes lógicos de un sistema informático que hacen posible que lleve a cabo tareas específicas. Por su parte, el *hardware* aparece como las partes físicas (tangibles) que acompañan a dicho sistema, esto es, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Así, el primero es el encargado de remitir las instrucciones y el segundo de ejecutarlas, de tal suerte que la interacción entre ambos es la que posibilita que un dispositivo funcione y sea operativo. En este marco, al conjunto de instrucciones que referíamos se les denominan algoritmos que son, en suma,

¹⁵ Fernández Hernández, C., Eguiluz Castañeira, J.A. (2024). Diez puntos críticos del Reglamento europeo de Inteligencia Artificial. *Diario LA LEY*, 85, 1-38.

¹⁶ Kaul, V.; Enslin, S. y Gross, S.A. (2020). History of artificial intelligence in medicine. *Gastrointestinal Endoscopy*, 92(4), 807-812.

los que permiten solucionar un problema¹⁷. Por otro lado, la robótica es una rama de diversos ámbitos científicos (como las ingenierías mecánica, electrónica y eléctrica) que se ocupa de diseñar, estructurar y construir un «robot»¹⁸.

Por tanto, podemos señalar que la inteligencia artificial es un «tipo» de *software*, pero que permite obtener resultados mucho más elevados y sofisticados, ya que utiliza redes neuronales y diversos enfoques y técnicas. En tal caso, disponemos de un programa que puede ser entrenado, que mejora continuamente y que puede tomar decisiones más o menos autónomas. Además, este sistema se puede incorporar a distintas máquinas para mejorar sus prestaciones. Así, por ejemplo, si se introduce en un robot podemos hablar de un robot inteligente, si se lleva a cabo en un vehículo estaremos frente a un vehículo autónomo o si se realiza en el seno de una aeronave tendremos un dron o un sistema de aeronave no tripulada¹⁹ (UAS).

— *Big data, IoT*. Por un lado, el funcionamiento adecuado de la inteligencia artificial precisa del tratamiento de grandes cantidades de datos, aumentando su rendimiento a medida que se incrementa el número de información facilitada. Claro es, no obstante, que se han de cumplir una serie de cautelas

¹⁷ A este respecto, destacan Čerka, P., Grigienė, J. y Sirbikytė, G. (2015). Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, 31 (3), 378 que la inteligencia artificial es diferente de los algoritmos informáticos convencionales, ya que tiene como objetivo convertirla en autodidacta (la capacidad de acumular experiencia personal) o con aprendizaje automático. Esta característica única permite actuar de manera diferente en las mismas situaciones, dependiendo de las acciones realizadas anteriormente, de forma muy similar a la experiencia humana. Las técnicas de modelado cognitivo y pensamiento racional dan más flexibilidad y permiten la creación de programas que pueden «comprender», es decir, que tienen los rasgos de una persona razonable (procesos de actividad cerebral).

¹⁸ Sobre el particular, destaca Zurita Martín, I. (2020). *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*. Reus, pp. 20-27 que, a pesar de la ausencia de unanimidad doctrinal, podemos concretar los requisitos esenciales que el mismo debe reunir, a saber, las capacidades de recoger datos mediante sensores, de procesar dichos datos en bruto y de planificar y cumplir acciones mediante conocimientos e información adquiridas. Por tanto, otras cualidades como la posibilidad de comunicación con un operador, con otros robots o con una red externa y el aprendizaje son circunstanciales. A este respecto, hemos de destacar la relevancia de la posibilidad de que los mismos accedan a la red de internet.

Por su parte, García-Prieto Cuesta, J. (2018). ¿Qué es un robot?. En *Derecho de los robots* (pp. 25-60). Wolters Kluwer, señala que la terminología empleada para definir a estas máquinas es algo ambigua. Así, indica el autor que se suele emplear de forma indistinta conceptos tales como robot, *bot*, *nanobot* o *softbot*. Desde esta perspectiva, los *nanobots* aparecen como una suerte de robots especialmente reducidos y los *softbots* como programas informáticos orientados a realizar tareas autónomas.

¹⁹ Para más información, *vid.* Castells i Marquès, M. (2019). Drones recreativos: normativa aplicable, responsabilidad civil y protección de datos. *Revista de Derecho Civil*, 6(1), 297-333; Torrubia Chalmeta, B. (2020). Aeronaves civiles no tripuladas. Contexto y regulación. En *Retos jurídicos de la inteligencia artificial* (pp. 255-267). Aranzadi.

en el ámbito de la protección de datos²⁰, por exigencia tanto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, como de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Igualmente, tenemos que destacar la incidencia del Internet de las Cosas (IoT, *Internet of Things*), que alude a la incorporación de internet, cada vez con más frecuencia, en diversos aparatos. A lo anterior, hay que anudar la interconexión que se produce entre todos estos dispositivos, lo que facilita el intercambio de datos y la interacción entre ellos (M2M, *machine to machine*). Sea como fuere, debemos incidir en la relevancia de disponer de bases de datos de entrenamiento adecuadas y que presenten una calidad aceptable. A este respecto, se ha de asegurar que son correctos y que no presentan deficiencias. Téngase en cuenta que esta información es la que procesa la inteligencia artificial, por lo que rápidamente podrá comprenderse la importancia de este extremo.

En relación con este aspecto, hemos de poner de relieve, a su vez, la significación de que exista una variabilidad considerable en cuando a la tipología de datos, toda vez que, de no ser así, las conclusiones que se obtengan estarán

²⁰ A este respecto, encontramos la primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial (STJUE de 7 de diciembre de 2023). En ella, se examina por primera vez el artículo 22 del RGPD sobre decisiones automatizadas. Aunque no aprovecha plenamente la ocasión, se establece un criterio garantista y expansivo que puede ser relevante especialmente respecto de las decisiones parcialmente automatizadas. Se sostiene que incluso puede tener futuras implicaciones para la consideración de sistemas de alto riesgo en la Ley de Inteligencia Artificial. Cabe destacar, asimismo, la Sentencia de la Corte Suprema de Chile de 9 de agosto de 2024 en la que se resuelve un asunto relacionado con las neurotecnologías. Más información en Cotino Hueso, L. (2024). La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial. *Diario LA LEY*, 80, 1-15.

Más recientemente, interesa destacar la STJUE 5 marzo 2024, C-755/2021 (LA LEY 25132/2024) que se ha pronunciado sobre el tratamiento ilícito de datos efectuado en el marco de la cooperación entre Europol y un Estado miembro y que da lugar a una responsabilidad solidaria entre ambos. Asimismo, es muy relevante la STJUE 7 marzo 2023, C-604/2022 (LA LEY 25140/2024) que ha resuelto un caso en el que se produjo una cesión de datos personales con fines publicitarios. En concreto, se trataba de una herramienta creada para registrar las preferencias de los usuarios, codificándolas en una cadena compuesta por una combinación de letras y caracteres que se comparte con intermediarios y plataformas publicitarias.

La importancia de la protección de datos personales puede comprobarse en el informe sobre la estrategia para Menores, Salud digital y privacidad, emitido por la Agencia Española de Protección de Datos (enero 2024) o en el *white paper* presentado por el Institute for Human-Centered Artificial Intelligence (HAI) de la Universidad de Stanford, «Rethinking Privacy in the AI Era - Policy Provocations for a Data-Centric World» (Repensando la privacidad en la era de la IA - Propuestas políticas para un mundo centrado en los datos), elaborado por Jennifer King, Privacy and Data Policy Fellow del HAI y Caroline Meinhardt, *policy research* manager del mismo.

sesgadas y podrán presentar falacias. En este sector, se hace referencia al sobreentrenamiento o sobreajuste (*overfitting*) que se produce cuando, como consecuencia de la entrada de demasiados datos y del ruido generado, el modelo de aprendizaje resulta preciso para los datos de entrenamiento, pero no ocurre de igual forma con respecto a datos nuevos.

— Capacidad de adaptación (aprendizaje), *machine learning* y *deep learning*. Asimismo, del uso de esta inteligencia se puede colegir que es capaz de aprender y mejorar a medida que se desarrolla el entrenamiento de la red neuronal. De este modo, el procesamiento continuo de los datos proporcionados conlleva que la máquina aprenda y mejore sus resultados. En este sentido, encontramos, al menos, tres tipos de aprendizaje: el aprendizaje supervisado, el aprendizaje no supervisado y el aprendizaje por refuerzo.

Surgen, pues, términos tales como el aprendizaje automático²¹ (*machine learning*) o el aprendizaje profundo²² (*deep learning*), que se refieren a los algoritmos que son capaces para aprender a partir de un conjunto de datos estructurados o a los que están basados en redes neuronales complejas que emulan el funcionamiento del cerebro humano para detectar patrones, respectivamente. Desde esta perspectiva, son capaces de elaborar predicciones y realizar tareas específicas.

Como ponen de manifiesto algunos autores²³, el *deep learning* es un tipo de *machine learning* que funciona mucho mejor con datos no estructurados y que permite que los modelos computacionales aprendan características progresivamente a partir de datos en múltiples niveles. Así, mientras que el aprendizaje del *machine learning* se mantiene estable al alcanzar el umbral de datos de entrenamiento, el *deep learning* aumenta y mejora su rendimiento a medida que incrementa la cantidad de datos. De esta suerte, se ha integrado en múltiples aplicaciones tales como el reconocimiento de voz e imagen de Google, los motores de recomendación de Netflix y Amazon, Siri de Apple, las

²¹ En este sentido, Garza-Ulloa, J. (2018). Chapter 6 - Application of mathematical models in biomechanics: artificial intelligence and time-frequency analysis. En *Applied Biomechanics using Mathematical Models* (pp. 373-524). Academic Press, señala que el aprendizaje automático puede ser definido como el proceso en el que los sistemas informáticos aprenden de los datos y utilizan algoritmos para ejecutar tareas sin estar programados explícitamente.

²² Para Wazid, M., Das, A.K., Chamola, V. y Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT express*, 8(3), 313-321, el aprendizaje profundo es una rama del aprendizaje automático basada en un conjunto de algoritmos que intentan modelar abstracciones de alto nivel en datos mediante el uso de múltiples capas de procesamiento, con estructuras complejas o no, compuestas por múltiples transformaciones no lineales.

²³ Mathew, A., Amudha, P. y Sivakumari, S. (2020). Deep Learning Techniques: An Overview. En *Advances in Intelligent Systems and Computing* (pp. 599-608). Springer.

respuestas automáticas de correo electrónico y texto y los chatbots²⁴ (estos últimos permiten simular una conversación con un profesional, con respuestas automatizadas).

— Autonomía. En definitiva, la incorporación de redes neuronales permite que las máquinas inteligentes desarrollen labores de forma autónoma, esto es, sin la intervención humana. En este sentido, a partir del aprendizaje basado en el procesamiento de los datos, pueden mejorar continuamente y resolver problemas. La interrelación de cantidades ingentes de datos sitúa en una posición idónea a la inteligencia artificial para escoger la opción que se presenta como la más adecuada, obtener conclusiones y perfeccionar el sistema.

Sin embargo, la verdadera enjundia no radica tanto en realizar interconexiones que permitan entrenar, aprender y, por tanto, actuar de forma autónoma. Muy al contrario, la dificultad estriba en diferenciar entre «casualidades» (correlaciones) y «causalidades», esto es, distinguir cuándo estamos ante un hecho que se presenta como una mera coincidencia, sin relación directa o indirecta y cuándo estamos ante un factor que influye en el resultado final. En suma, consiste en desechar las correlaciones que no tienen incidencia y que, en consecuencia, no implican causalidad.

En el caso contrario, la máquina estaría utilizando datos que no son relevantes, que distorsionan el análisis y producen disfuncionalidades. De ello, pues, se deriva un mal funcionamiento de la inteligencia artificial. Un efecto parecido al que anteriormente aludimos en relación con la sobreinformación, ya que impide un examen adecuado. Como ejemplo, podemos referenciar la inteligencia artificial que utilizaba Amazon para contratar personal, la cual, sin saber concretamente el motivo, tenía un sesgo sexista y descartaba los currículums vitae de las mujeres.

De hecho, la escasa normativa española que, en cierta medida, regula la inteligencia artificial se ocupa, precisamente, la igualdad de trato y no discriminación en el ámbito de la inteligencia artificial y mecanismos de toma de decisión automatizados, implementando criterios de minimización de sesgos. *Vid.*, a modo de ejemplo, el artículo 23 de la Ley 15/2022, de 12 de julio,

²⁴ A este respecto, destacan Kaul, V.; Enslin, S. y Gross, S.A. (2020). History of artificial intelligence in medicine. *Gastrointestinal Endoscopy*, 92(4), 807-812, que el aprendizaje automático supone el uso de rasgos específicos para identificar patrones que pueden usarse para analizar una situación particular y que la máquina pueda «aprender» y aplicar esa información a futuros escenarios similares. Por su parte, el avance de esta tecnología ha dado lugar al aprendizaje profundo, que se compone de algoritmos para crear una red neuronal artificial (RNA) que puede aprender y tomar decisiones por sí sola, de una forma similar al cerebro humano.

integral para la igualdad de trato y la no discriminación²⁵ o el Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura.

— Los *outputs* del sistema: predicciones, contenidos, recomendaciones o decisiones. Tal y como señala la Ley de Inteligencia Artificial, los sistemas de inteligencia artificial ofrecen diferentes resultados en función tanto de la programación que tengan como del uso que se pretenda obtener. Así pues, este hecho permite diferenciar entre los diversos sistemas existentes: la inteligencia artificial generativa, permite generar textos, imágenes u otros contenidos; por su parte, la inteligencia artificial predictiva, partir de la información incorporada y el aprendizaje automático, identificar patrones pasados y realizar predicciones futuras.

— Oscuridad, *Black Box*. Otro rasgo definitorio de la inteligencia artificial es el gran desconocimiento existente en relación con su funcionamiento. Es decir, resulta muy complejo determinar cómo procesa la información y cómo alcanza la decisión concreta debido a la interacción no lineal entre neuronas y capas, y la alta dimensionalidad de los datos. Por este motivo, se habla de cajas negras²⁶ para poner de relieve la dificultad (en ocasiones, incluso, imposibilidad) a la hora de concretar el «razonamiento» que ha seguido el software para alcanzar la conclusión propuesta.

A lo anterior, hay que anudar las reticencias de los desarrolladores de estas redes neuronales a ofrecer datos al respecto, esto es, a que se pueda acceder al interior de la inteligencia. En este sentido, no se puede perder de vista que pueden confluír otros derechos (como la protección de datos, los secretos industriales, patentes, propiedad intelectual²⁷, etc.) que podrían verse comprometidos si se expusiera al público.

²⁵ Acerca de esta norma, *vid.* FERNÁNDEZ HERNÁNDEZ, C. (2022). La Ley 15/2022 introduce la primera regulación positiva de la inteligencia artificial en España. *Diario La Ley*, (64), 1-8. Como señala el autor citado, esta norma, que «contiene la primera regulación positiva del uso de la inteligencia artificial por las administraciones públicas y las empresas en nuestro país», es «una regulación programática y en cierto modo voluntarista, que diseña unas grandes líneas de actuación de las administraciones públicas, con el objetivo de «favorecer», «promover» y «priorizar» determinadas políticas y prácticas relacionadas con el uso de «algoritmos involucrados en la toma de decisiones».

²⁶ En este sentido, en cuanto a los desafíos de la inteligencia artificial en medicina, Kulkarni, S., Seneviratne, N., Baig, M.S. y Ahmed Khan, A.H. (2020). Artificial Intelligence in medicine: where are we now?. *Academic Radiology*, 27(1), 62-70, incluyen el problema de la caja negra y el sobreajuste, entre otros.

²⁷ Cabe reseñar que el pasado día 14 de marzo de 2024 y tal como se acordó con el Consejo el 5 de diciembre de 2023, el Parlamento Europeo ha aprobado la propuesta de un Reglamento para la modificación del Reglamento (CE) 6/2002 del Consejo, de 12 de diciembre de 2001, sobre los dibujos y modelos comunitarios (COM(2022) 666 final) y de una Directiva del Parlamento Europeo y del Consejo sobre la protección jurídica de los dibujos y modelos (refundición) (COM(2022) 667 final), presentados por la Comisión en noviembre de 2022.

A partir de este breve análisis de los caracteres fundamentales de la inteligencia artificial, podemos concluir que estamos ante realidades diferentes a la robótica tradicional en la medida en que su funcionamiento y las tareas que lleva a cabo no se asemejan a las desarrolladas por esta última. En realidad, una de las razones esenciales de esta idea es que encontramos, en cierta medida, una pérdida de control por parte del ser humano. Así, a pesar de que no estemos en un estadio definitivo en el que las máquinas operen de forma totalmente autónoma, el aprendizaje y la mejora continua a partir del procesamiento de cantidades muy elevadas de datos permiten que estas redes obtengan deducciones de forma autárquica.

2.2. EL RIESGO Y LA INTERVENCIÓN HUMANA: LAS ACTIVIDADES PROHIBIDAS Y LA CLASIFICACIÓN DE LOS SISTEMAS

Íntimamente ligado a lo anterior, aparece el tema relativo al riesgo que conlleva el sistema de inteligencia artificial. Este último aparece configurado en la Ley de Inteligencia Artificial como una combinación entre la probabilidad de que se produzca un daño y la gravedad que presente el mismo. Sobre el particular, hemos de efectuar las siguientes consideraciones. Por un lado, por obvio que parezca, hay que señalar que los perjuicios a los que se refiere se centran en la salud y la seguridad de las personas y de los bienes. En términos generales, se ocupa de riesgos potenciales para los derechos subjetivos de las personas, englobando las distintas tipologías.

Así pues, se puede deducir que cabe reclamar los daños producidos a la vida y a la integridad de las personas, así como a otros bienes de la personalidad (como, por ejemplo, los datos personales, el honor, la intimidad y la propia imagen). Asimismo, se pueden reclamar todos aquellos que se manifiesten contra los bienes físicos o intangibles y que produzcan un menoscabo. Además, desde nuestra perspectiva, la indemnización de daños y perjuicios que, en su caso, corresponda, incluirá tanto el daño emergente (efectivamente producido), como el lucro cesante (beneficios que se dejan de percibir como consecuencia del sistema de inteligencia artificial) e, incluso, los daños morales (siempre que sean probados por algún medio admitido en Derecho y que sean cuantificados).

Por otro lado, conviene que nos centremos en la delimitación de los dos elementos que configuran el riesgo. Por lo que respecta a la probabilidad y como no puede ser de otro modo, se determina en relación con un concepto indeterminado e impreciso por naturaleza. En otras palabras, no es posible llevar a cabo una concreción exacta en términos absolutos, sino que, a través de indicios (y presunciones) se escoge aquella opción que, a priori, se presen-

ta como más probable. Ello no quiere decir que este hecho convierta el riesgo en una cuestión arbitraria. Nada más lejos de la realidad. Simplemente hay que tener en cuenta que, ante la ausencia de certezas y de datos suficientes, es necesario realizar una estimación lo más aproximada posible de la realidad del sistema y evaluar las posibilidades de que produzca un daño a terceros.

Igualmente, en la definición de la probabilidad del riesgo aparece implícito un criterio para tener en cuenta y que ya se encontraba en otros textos europeos. Nos referimos a la consideración de la intervención humana como herramienta para reducir dicha probabilidad o, en caso contrario, para aumentarla. Esta disquisición, como se puede comprobar, se encuentra ligada, a su vez, con la consideración de la autonomía de los sistemas, de tal suerte que: a mayor autonomía del sistema, menor intervención del humano y, por tanto, mayor riesgo; y, a la inversa, a menor autonomía de los sistemas, mayor intervención del humano y, en consecuencia, menor riesgo.

De hecho, esta posición se ve reforzada (esta vez, de forma explícita) en diversos preceptos de la Ley de Inteligencia Artificial. *Vid.*, por ejemplo, el artículo 7.2 d) y el artículo 14 que está dedicado, precisamente, a la supervisión humana. Para obtener una conclusión de estas características, entendemos que, al menos, se tendría que haber llevado a cabo un estudio profundo del funcionamiento de los sistemas, en función del ámbito en el que actúen y la propia autonomía que tengan. Asimismo, consideramos que tal examen viene condicionado por el entorno, esto es, no es equiparable un contexto en el que solamente interactúen sistemas a otro en el que se combine la actuación de este último con la de los humanos. Sin duda, el primero genera un riesgo menor que el segundo y este elemento resulta fundamental para tomar una decisión al respecto.

En cuanto a la gravedad, hemos de advertir que tiene dos vertientes; una cuantitativa y otra cualitativa. En la primera, se toma en consideración el número de personas y/o de bienes que serían afectados en el caso de producirse el evento adverso. En la segunda, se dilucida sobre el tipo de bien jurídico en cuestión y se trata, en la medida de lo posible, de hacer una suerte de prelación. En este sentido, parece evidente que los derechos fundamentales ocupan una posición de preeminencia y su conculcación es la más trascendental. No obstante, no resulta sencillo, por ejemplo, llevar a cabo una clasificación de importancia entre estos derechos. Tampoco se presenta como una tarea fácil diferenciar entre otros bienes jurídicos que, sin ser fundamentales, representan un ámbito protegido por el ordenamiento jurídico (piénsese en los daños producidos en los bienes). Más tarde volveremos sobre estas disquisiciones.

Sea como fuere, lo cierto es que el riesgo es esencial en la Ley de Inteligencia Artificial, al menos, para dos extremos. En primer lugar, para

establecer las actividades que se consideran vetadas por ser contrarias a los principios y valores de la Unión Europea. Son las que el artículo 5 de la Ley de Inteligencia Artificial denomina prácticas de inteligencia artificial prohibidas y que están íntimamente relacionadas con los derechos fundamentales a los que antes aludíamos. A modo de ejemplo, no están permitidos los sistemas que tratan de manipular la conducta de las personas de forma subliminal, los que exploten las vulnerabilidades de determinados grupos (como menores de edad o personas con discapacidad), que clasifiquen a los particulares en atención a su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual, o que los identifiquen de forma biométrica a distancia en tiempo real en espacios de acceso público con fines policiales (con las salvedades oportunas).

En segundo lugar, en el ámbito de las actividades que, en principio, están permitidas, el riesgo adquiere vigencia para la clasificación de los sistemas y, en particular, para determinar aquellos que son de alto riesgo. Repárese que este extremo tiene una importancia vital, pues de ello se derivará la aplicación de unas reglas u otras. No obstante, el artículo 6 de la Ley de Inteligencia Artificial, en una compleja redacción, anuda otro criterio para valorar dicha clasificación. Nos referimos a los sectores concretos en los que va a operar el sistema de inteligencia artificial (ya sea como un componente de los productos, ya como un producto en sí mismo) y que vienen concretados en los anexos I y III de la norma.

Por lo que se refiere al anexo I, prevé el apartado 1 del mencionado precepto que se deben cumplir dos condiciones: que el sistema esté destinado a utilizarse como componente de seguridad de un producto, o el sistema sea en sí mismo un producto, cubierto por la legislación de armonización de la Unión enumerada en el anexo I; y que el producto deba someterse a una evaluación de conformidad con arreglo a esta última legislación. Pues bien, el anexo I contempla diversas normativas entre las que cabe citar las relativas a máquinas, a la seguridad de los juguetes, a las embarcaciones de recreo y motos acuáticas y a los ascensores y componentes de seguridad para ascensores.

En otro orden de cosas, el artículo 6.2 de la Ley de Inteligencia Artificial se refiere a los sistemas contemplados en el anexo III. En este sentido, este último contempla siete ámbitos diferentes: los datos biométricos, las infraestructuras críticas (como el tráfico rodado o el suministro de agua), la educación y formación profesional, el acceso y disfrute de los servicios y prestaciones esenciales de carácter privado o público (tales como asistencia pública, solvencia crediticia o seguros de vida), las fuerzas y cuerpos de seguridad, la gestión de la migración, el asilo y el control de fronteras y la administración de justicia y procesos democráticos. En todo caso, en muchos de ellos su uso está condi-

cionado a que esté permitido en la legislación nacional de que se trate, pues en caso contrario no estaríamos ante un sistema de alto riesgo, sino ante una actividad prohibida.

En todo caso, la clasificación de un sistema como de alto riesgo tiene importantes consecuencias prácticas, pues se deriva un régimen más estricto y taxativo en tal escenario en la Ley de Inteligencia Artificial. En definitiva, dado el potencial peligro que genera (o puede generar) para los derechos subjetivos, el legislador ha querido establecer mecanismos que eliminen o, al menos, reduzcan, las posibilidades de que se manifiesten estos daños (*vid.*, a modo de ejemplo, el art. 15 Ley Inteligencia Artificial sobre precisión, solidez y ciberseguridad).

Así ocurre, por ejemplo, con la exigencia del sistema de gestión de riesgos, así como con su revisión y actualización periódica y sistemática. En este marco, pues, tendrán que ser identificados, analizados y evaluados los riesgos que puedan surgir tanto si se utiliza de acuerdo con su finalidad prevista como si se trata de un uso indebido. Asimismo, es preciso que se adopten las medidas adecuadas y específicas para hacer frente a dichos riesgos y contemplar medidas de actuación.

Desde esta perspectiva, la Ley de Inteligencia Artificial divide los sistemas en cuatro categorías²⁸, en función de sus capacidades y los riesgos para la salud y la seguridad que entraña, así como para los derechos fundamentales de las personas:

- Sistemas de inteligencia artificial de riesgo mínimo: como videojuegos que integren esta tecnología y filtros de spam.
- Sistemas de inteligencia artificial de riesgo limitado: donde encontramos, por ejemplo, los chatbots.
- Sistemas de inteligencia artificial de alto riesgo: como sistemas robóticos de selección de personal o sistemas para evaluar la solvencia de las personas y establecer una clasificación crediticia.
- Sistemas de inteligencia artificial con un riesgo inasumible o inaceptable: sistemas de categorización social para la supervisión de la sociedad o sistemas de identificación biométrica para expandir o crear bases de datos de reconocimiento facial.

A este respecto, conviene tener en cuenta varias cuestiones. Por un lado, que en otros instrumentos normativos anteriores la consideración de alto ries-

²⁸ En este punto, *vid.* el número 661 de la revista *Computer Hoy*, disponible en: <https://computerhoy.com/tecnologia/ya-quiosco-numero-661-computer-hoy-1359556> (fecha de última consulta: 01.07.2024).

go se acompañaba de la exigencia de un seguro obligatorio y de una responsabilidad objetiva y que, al margen de que más tarde volvamos sobre estas consideraciones, no ocurre algo similar en la Ley de Inteligencia Artificial. Por otro lado, aparecen los denominados organismos notificados²⁹ que se constituirán con arreglo al Derecho nacional y cuya función es evaluar la conformidad del sistema de inteligencia artificial de alto riesgo. Llama la atención, por lo demás, que en este caso el artículo 31.9 de la Ley de Inteligencia Artificial sí incorpora la necesidad de que estos organismos suscriban un seguro de responsabilidad civil apropiado (a menos que la responsabilidad sea asumida por el Estado miembro en el que estén establecidos o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad).

Íntimamente ligado con lo anterior, la Ley de Inteligencia Artificial contempla disposiciones relativas a los datos y a la gobernanza de los mismos, desde una doble perspectiva. En primer lugar, para que los sistemas que entrenen con modelos de datos se desarrollen sobre unas bases de calidad y que no estén sesgados o contaminados. En segundo lugar, se pretende que los sistemas de inteligencia artificial sean transparentes.

Esto último, se materializa en la documentación técnica que debe elaborarse (art. 11 Ley Inteligencia Artificial), en el mantenimiento de registros automáticos (art. 12 Ley Inteligencia Artificial) y en las propias instrucciones de uso que acompañen al sistema y que permitan que se haga un uso responsable (art. 13 Ley Inteligencia Artificial). En suma, que los usuarios conozcan las características, capacidades, limitaciones y finalidad del sistema y que exista una trazabilidad adecuada en orden a detectar el origen del error o del daño producido.

Hemos de aludir a que esta circunstancia está ligada a otras cuestiones que tendremos ocasión de señalar como la supervisión humana y la depuración de responsabilidad, ya que su incumplimiento, además de las sanciones oportunas, podrá comportar el recurso a las correspondientes presunciones en sede de responsabilidad civil. Y es que, la intervención y la supervisión humana se emplea también para delimita otro concepto esencial: el control. En este sentido, desde nuestra perspectiva, la Unión Europea trata de lograr un doble objetivo. De un lado, asegurar que siempre exista un sujeto responsable (a poder ser, radicado en territorio europeo) para responder del daño causado. De otro lado, intentar que el resarcimiento se lleve a cabo por la persona

²⁹ También cabe aludir a la Oficina de Inteligencia Artificial, que ya ha sido creada por la Comisión Europea y cuya misión será supervisar los modelos de inteligencia artificial, incluidos los de propósito de propósito general, así como la interacción con la comunidad científica, desempeñando un papel clave en las investigaciones y pruebas de esta tecnología y en la aplicación del Reglamento.

que, en realidad, puede evitar o minimizar el resultado dañoso (lo cual evoca, por lo demás, a la propia responsabilidad subjetiva o por culpa).

En el primer caso, tal extremo se puede comprobar en la exhaustiva enumeración que efectúa el artículo 2.1 de la Ley de Inteligencia Artificial, que se refiere a los proveedores que comercialicen o pongan en servicio los sistemas o que introduzcan en el mercado modelos de IA de uso general³⁰ en la Unión, a los proveedores y responsables del despliegue, a los importadores y distribuidores, a los fabricantes y a los representantes autorizados. Y este listado tiene otras manifestaciones en el articulado posterior, tal y como ocurre con el artículo 8.2 que destaca que «los proveedores serán responsables de garantizar que su producto cumple plenamente todos los requisitos aplicables exigidos en virtud de la legislación de armonización de la Unión que sea aplicable». A ello, hay que anudar los ya mencionados organismos notificados y, como no puede ser de otro modo, los propios usuarios finales (consumidores) y el uso que hagan del sistema.

3. LA RESPONSABILIDAD CIVIL DERIVADA DEL USO DE SISTEMAS INTELIGENTES

3.1. LAS RELACIONES ENTRE LAS DOS PROPUESTAS DE DIRECTIVA

En este punto, es preciso que, antes de adentrarnos en el régimen jurídico aplicable, tratemos de esclarecer el ámbito de aplicación de las dos herramientas a las que hemos aludido³¹: la propuesta de Directiva sobre productos defectuosos (aprobada por el Parlamento Europeo el 12 de marzo de 2024) y la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial. No obstante, hay que

³⁰ En todo caso, como pone de relieve, BARRIO ANDRÉS, M. (2024). Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial. *Diario La Ley*, 86, 1-6, la regulación de los modelos y sistemas de inteligencia artificial de uso general (GPAI), no es coherente, toda vez que establece las obligaciones específicas sin atender a un enfoque basado en el riesgo (en la medida en que regulan una determinada tecnología en lugar de riesgos concretos). Además, la categoría de «riesgo sistémico» tampoco se basa en pruebas empíricas, sino que es el resultado de un compromiso político.

³¹ Como pone de relieve Reyes López, M.J. (2023). La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias. *Actualidad Civil*, (7), la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial «complementa la nacida para regular la responsabilidad por productos defectuosos armonizando normas aplicables a las reclamaciones que quedan excluidas de su ámbito de aplicación en los casos en que los daños sean debidos a un comportamiento ilícito».

tener en cuenta que esta última no resuelve el problema de la responsabilidad civil, sino que incorpora una serie de reglas para revisar las disposiciones de los distintos estados en aras de favorecer la reparación integral de las víctimas.

Así, se plantea entonces cómo operan ambos instrumentos normativos. En otras palabras, parece que se solapan y que responden a una misma realidad. En suma, una vez que, partiendo de la definición de la Ley de Inteligencia Artificial llegamos a la conclusión de que estamos ante un producto inteligente, si suponemos que este último causa un daño, ¿aplicamos la propuesta de Directiva de responsabilidad civil por productos defectuosos o la propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial?

Por un lado, si el daño se produce, a pesar de cumplir con las medidas de seguridad previstas en la legislación europea (o al margen de las mismas), como resulta lógico, se ha de recurrir a la legislación del estado en cuestión para ventilar la responsabilidad. A este respecto, del estudio efectuado por la Comisión, se concluye que la mayoría son sistemas basados en la culpa. Sea como fuere, si bien esta regla se mantiene inmutable, como regla general, en el ámbito contractual, existe un matiz en el Derecho de daños. Así las cosas, en este último escenario adquiere especial vigencia la Propuesta Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, toda vez que supondrá una revisión de la carga probatoria de las normativas nacionales de responsabilidad civil. En otras palabras, los tribunales de los estados, al resolver los pleitos sobre responsabilidad, aplicarán las respectivas disposiciones nacionales, pero teniendo en cuenta las reglas y presunciones de la mencionada propuesta de Directiva.

En todo caso, hay que tener en cuenta que los estados miembros deberán aprobar leyes de transposición de la propuesta de Directiva y, al efectuar esta tarea, se permite que establezcan una mayor protección para las víctimas. En este sentido, la propuesta de Directiva es de mínimos, lo que no impide que se incorpore un régimen más tuitivo en favor de los perjudicados (lo cual podría suponer, incluso, la previsión de una responsabilidad objetiva).

Por otro lado, si el daño tiene ocasión como consecuencia del incumplimiento de las medidas de seguridad, resultan potencialmente aplicables tanto la Propuesta Directiva sobre productos defectuosos como las legislaciones nacionales (acordes, eso sí, con la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial). Para resolver esta duplicidad y aparente solapamiento, se determinan dos reglas; a saber, en primer lugar, tendremos que acudir a la propuesta de Directiva sobre productos defectuosos y, para aquellas personas no previstas (cuando, por ejemplo, la víctima no tiene la condición de consumidor o usua-

rio³²) o para los daños no contemplados (como el sector contractual) en la misma, resultarán vigentes las normas de los estados miembros y la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (o, de existir, la legislación europea especial).

Por lo que se refiere a la Propuesta Directiva sobre productos defectuosos, cabe señalar que también será necesario que los estados dispongan de normas de transposición y, a diferencia de la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, su artículo 3 impide que las legislaciones nacionales se aparten de lo contemplado en ella (con independencia de que se lleve a cabo para incluir un régimen más o menos protector). Así, se busca alcanzar un nivel de amparo de los consumidores equivalente en todos los países³³. Por ello, se plantea la posible revisión, en su caso, del Real Decreto Legislativo 1/2007, de 16 de noviembre.

En relación con la aplicación de ambas propuestas de Directiva, indica la doctrina³⁴ que la propuesta de Directiva sobre productos defectuosos tiene un ámbito distinto, pues se refiere a cualesquiera tipos de productos (no sola-

³² En este punto, hay que tener en cuenta que la enmienda 172 ha modificado el artículo 3.1 punto 4 relativo a la figura del entonces «usuario», ya que pasa a denominarse «implementador». Este último, pues, aparece como «toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional». Entendemos que este cambio favorecerá la claridad conceptual y evitará confusiones con otras figuras como los consumidores y usuarios. Así las cosas, como destaca el artículo 3.1 punto 8 bis (enmienda 174), cuando se produzca un daño estaremos ante una «persona afectada».

³³ Como pone de relieve Rodríguez De Las Heras Ballell, T. (2023). La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial. *LA LEY mercantil*, (103), «la revisión de la Directiva sobre responsabilidad por productos defectuosos desempeña un papel clave, con un potencial armonizador que probablemente supere el efecto tradicional y formal de una Directiva». Así las cosas, al «ampliar el ámbito de aplicación de la Directiva sobre responsabilidad por productos defectuosos para incluir los bienes que utilizan inteligencia artificial y los sistemas de IA, y al adaptar algunas normas a las características de dichos sistemas, se refuerza, amplía y aprovecha el potencial de armonización de la Directiva sobre responsabilidad por producto: aunque esto implique proceder mediante una directiva, se trata de una directiva con una cláusula expresa de armonización plena».

Asimismo, Astray Chacón, M.P. (2023). Daños causados por la inteligencia artificial. *Actualidad Civil*, (7), destaca que la adaptación normativa, que se impone como necesaria, se proyecta sobre tres instrumentos de armonización: «la propuesta de Reglamento 2021, la propuesta de Directiva sobre responsabilidad civil extracontractual de la IA y la propuesta de revisión de la Directiva sobre responsabilidad por los daños causados por productos defectuosos».

³⁴ Atienza Navarro, M. L. (2023). ¿Una nueva responsabilidad por productos defectuosos?, Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495). *InDret: Revista para el Análisis del Derecho*, (2), 5.

mente los que integren inteligencia artificial) y requiere que adolezcan de un defecto.

Y es que la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial complementa la nacida para regular la responsabilidad por productos defectuosos armonizando normas aplicables a las reclamaciones que quedan excluidas de su ámbito de aplicación en los casos en los que los daños sean debidos a un comportamiento ilícito. Sin embargo, algunos autores³⁵ cuestionan esta «complementariedad» entre ambas propuestas, al plantear el debate acerca de extender la responsabilidad objetiva a todos los supuestos (máxime cuando el demandante sea consumidor).

A nuestro entender, lo más adecuado hubiera sido que ambas propuestas de Directiva optasen por una misma solución, es decir, por recurrir a un sistema más rígido que limite la potestad legislativa nacional (siguiendo la propuesta de Directiva sobre productos defectuosos) o, por el contrario, incorporar un régimen que reconozca un mayor intervencionismo nacional (tal y como efectúa la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial). Y es que, desde nuestra perspectiva, no parece que existan motivos suficientes para establecer una protección desigual en atención a la defectuosidad de un producto o a la condición (de consumidor o no) de la víctima. Muy al contrario, si se desea favorecer el resarcimiento integral (lo cual, por otro lado, resulta legítimo), debería ser equivalente en todos los supuestos de responsabilidad civil derivada del uso de la inteligencia artificial. En suma, promover que los sistemas que integren esta tecnología sean seguros y que, si aun así se produce un perjuicio, que los afectados cuenten con una cobertura completa.

Asimismo, la «convivencia» entre ambas propuestas de Directiva tampoco se ve favorecida si atendemos al tipo de responsabilidad que incorporan (objetiva en la propuesta de Directiva sobre productos defectuosos y subjetiva en la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial). A este respecto, observa la doctrina³⁶, muy acertadamente, que si bien las dos propuestas de Directiva pretenden consolidar un sistema general de responsabilidad civil eficaz, tal y

³⁵ Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 7-9.

³⁶ Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 7-9.

como están planteadas «la relación y conjugación entre ambas propuestas no parece sencilla».

Una de las cuestiones esenciales sobre las que giran estas propuestas es la dificultad probatoria con la que se puede encontrar la víctima a la hora de demostrar los elementos alegados en la demanda. Entre otros, la culpa del agente que circula un sistema inteligente, su funcionamiento deficiente, el nexo causal e, incluso, el daño causado. Asimismo, otro inconveniente que adquiere vigencia en este campo es la multiplicidad de sujetos que actúan y que, por tanto, podrían ser catalogados como potenciales responsables.

Desde esta perspectiva, ambos instrumentos tratan de resolver estas disquisiciones. En el caso de la propuesta de Directiva de responsabilidad civil por productos defectuosos, la culpa no supone un verdadero problema en tanto en cuanto incorpora un régimen objetivo de responsabilidad. El tema central radica en la defectuosidad del producto y en la causalidad. En este sentido, si el artículo 6 de la propuesta de Directiva prevé cuándo estamos ante un producto defectuoso, los artículos 8 y 9, mediante la atribución del deber de exhibir pruebas al demandado y de los requisitos de las normas sobre seguridad, incorporan una serie de presunciones tanto de la defectuosidad como del nexo causal.

Así, en términos generales y con algunos matices, se puede deducir que, cuando el demandante no cumpla con la citada obligación (de exhibición), se presumirá que estamos ante un producto defectuoso y que existe una relación directa (nexo) entre este último y el perjuicio causado. Por lo que se refiere a los sujetos responsables, la propuesta de Directiva de responsabilidad civil por productos defectuosos introduce varias reglas de atribución de responsabilidad para asegurar que la víctima siempre pueda tener un operador en la Unión Europea al que dirigirse. Además, estas se aplican de forma preferente y subsidiaria, es decir, el primer llamado a resarcir el daño es el fabricante; en su defecto (cuando esté establecido fuera de la Unión), el importador y el representante autorizado; en su defecto, el prestador de servicios de tramitación de pedidos a distancia; y así sucesivamente. A ello, hay que anudar el mantenimiento de la responsabilidad solidaria que ya venía en la versión originaria de la Directiva.

En el supuesto de la propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial y por más que nos ocupemos con más detalle posteriormente, conviene destacar que también incluye reglas para paliar estos efectos negativos. Igualmente, en este escenario aparece una problemática particular, ya que el recurso a la responsabilidad subjetiva conlleva que el demandante también tenga que

probar la culpa. Por este motivo, se incluyen en esta propuesta algunas disposiciones sobre el particular, como veremos.

En este punto, hemos de señalar, siguiendo las palabras de la doctrina, que, dado que la Ley de Inteligencia Artificial no regula la responsabilidad civil nacida de inteligencia artificial, se hace necesario establecer normas que contemplen el impacto de los daños generados por productos creados por estos sistemas, pues la normativa vigente tampoco es suficiente para afrontar esta nueva realidad³⁷.

A este respecto, la primera cuestión que hemos de señalar es que, en realidad, la propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial no supone una regulación «completa» del derecho de daños. Al contrario, esta resulta aplicable cuando tengamos que recurrir a las legislaciones nacionales. Desde esta perspectiva, aparece como un complemento de estas últimas; si se quiere, esta propuesta de Directiva tiene como función «aligerar» la carga probatoria del demandante e introducir una serie de presunciones, pero no establece un tipo de responsabilidad concreta. Así pues, los tribunales de los estados, al resolver los pleitos sobre responsabilidad, aplicarán las respectivas disposiciones nacionales, pero teniendo en cuenta las reglas y presunciones de la mencionada propuesta de Directiva.

3.2. LA RESPONSABILIDAD CIVIL EN LA (REVISADA) PROPUESTA DE DIRECTIVA SOBRE PRODUCTOS DEFECTUOSOS

Para comenzar, interesa resaltar, con carácter previo, que, al margen de las críticas que pueden efectuarse por la excesiva antelación del Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, su aprobación pone de relieve que estamos ante la estrategia europea definitiva (en la que, por lo demás, también se inserta el Plan de Recuperación, Transformación, y Resiliencia, para dar cumplimiento al Pacto por la Ciencia y la Innovación, y en el que se enmarca la Estrategia Nacional de Inteligencia Artificial). Así, a Ley de Inteligencia Artificial³⁸ se suman la (revisada) Directiva sobre produc-

³⁷ A este respecto, Reyes López, M.J. (2023). La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias. *Actualidad Civil*, (7).

³⁸ A este respecto, destaca Reyes López, M.J. (2023). La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias. *Actualidad Civil*, (7), que «La propuesta de reglamento no regula la responsabilidad civil nacida de IA, por lo que se hace necesario establecer normas que contemplen el impacto de los daños generados por productos creados por IA dado que la normativa vigente tampoco es suficiente para afrontar esta nueva realidad».

tos defectuosos y la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial³⁹.

De hecho, estos dos instrumentos toman como referencia el propio concepto de sistema de inteligencia artificial que incorpora este último instrumento, así como la clasificación de los sistemas y los requisitos, criterios y obligaciones previstos en la Ley de Inteligencia Artificial. En todo caso, a diferencia de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial de 2020, la clasificación de la Ley de Inteligencia Artificial no conlleva la adscripción de una responsabilidad objetiva. Muy al contrario, se parte de un tipo concreto de responsabilidad, con la aplicación, en su caso, de la presunción de algunos elementos como la culpa.

3.2.1. Reflexiones acerca del concepto de producto defectuoso y los sujetos responsables

Una vez esclarecida la cuestión anterior, corresponde que nos adentremos, con algo más de detalle, en la regulación concreta de la propuesta de Directiva sobre productos defectuosos. La finalidad última de esta disposición es proporcionar un sistema, a escala de la Unión Europea, que resulte satisfactorio a la hora de compensar a las personas que sufran lesiones físicas o daños materiales debido a productos defectuosos. Este objetivo, que es compartido con la versión original de 1985, se ha visto alterado por los cambios producidos en la manera que se fabrican, distribuyen y funcionan los productos, así como por la propia modernización de las normas de seguridad. En especial, la incidencia del entorno digital y, en su seno, de la inteligencia artificial, justifica una revisión de determinados aspectos que han quedado obsoletos y que no parecen acoger las nuevas realidades (*vid.*, por ejemplo, el propio concepto de producto defectuoso). En suma, se busca establecer normas de responsabilidad que se ajusten a la transición verde y digital.

Este último aspecto, unido a la dificultad existente en relación con la carga probatoria y con la excesiva limitación en las reclamaciones por indemnización de daños y perjuicios, son calificadas en la Exposición de Motivos de la Propuesta Directiva sobre productos defectuosos como «deficiencias» que han de ser mejoradas. Además, estas disquisiciones ya se advertían en otras disposiciones emitidas con anterioridad (como el Libro Blanco sobre la Inteligencia Artificial o el informe del Grupo de Expertos sobre Responsabilidad Civil y

³⁹ Para más información, *vid.* MARTÍN-CASALS, M.: «La regulación de la responsabilidad extracontractual por daños causados por sistemas de inteligencia artificial (IA) mediante dos propuestas de directiva», *Revista de responsabilidad civil, circulación y seguro*, 2023, núm. 1, pp. 6-30.

Nuevas Tecnologías). Por su parte, otras cuestiones que son muy relevantes y que preocupan a la Comisión son, por un lado, asegurar que siempre exista una empresa con sede en la Unión Europea que pueda ser considerada responsable de los productos defectuosos comprados directamente a fabricantes situados fuera de la misma (operadores económicos⁴⁰).

Por otro lado, se persigue ampliar el campo de sujetos potencialmente responsables, incluyendo no solamente a los fabricantes (*hardware manufacturer*), sino también a los proveedores (o desarrolladores) de programas informáticos o de sistemas de inteligencia artificial (*software manufacturer*) que influyan en el funcionamiento del producto⁴¹. Igualmente, se pretende establecer un equilibrio justo entre los operadores económicos y los consumidores (tal y como se contempla, de hecho, en las conclusiones y recomendaciones del Dictamen del Comité Económico y Social Europeo sobre Revisión de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, aprobado en pleno de 24 de enero de 2023).

Para ofrecer una respuesta adecuada, lo primero que realiza la propuesta Directiva sobre productos defectuosos es confirmar que los sistemas de inteligencia artificial y los bienes basados en la misma son productos y, por tanto, entran en su ámbito de aplicación. Como consecuencia inmediata, contempla una definición más amplia y actualizada de producto en su artículo 4.1⁴²,

⁴⁰ En este sentido, el artículo 8 establece diversas reglas para asegurar que la víctima contará con un sujeto responsable al que dirigir la reclamación. De una forma gráfica: En primer lugar, la responsabilidad recae sobre el fabricante (donde se engloba, además, a toda persona física o jurídica que modifique de forma sustancial un producto ya introducido en el mercado). Cuando el fabricante esté establecido fuera de la Unión, se acude al importador y al representante autorizado del fabricante. En su defecto (esto es, cuando también estén establecidos fuera de la Unión) los dos sujetos anteriores, se ventilará la responsabilidad del prestador de servicios de tramitación de pedidos a distancia. Sea como fuere, esta previsión no afecta a la exención de responsabilidad prevista en el Reglamento sobre servicios digitales. Si no puede identificarse a ninguno de los anteriores, podrá declararse la responsabilidad del distribuidor cuando el demandante le solicite que identifique al operador económico o persona que le suministró el producto y no lo lleve a cabo en el plazo de un mes. Incluso, en aquellos supuestos en los que no estén bajo el control del fabricante, adquiere vigencia la figura del proveedor del servicio conexo.

⁴¹ Para parte de la doctrina, este hecho conlleva la atribución de la condición de productor a todos ellos. De hecho, la necesidad de esta ampliación de sujetos responsables ya se destacaba por algunos autores. Por todos, *vid.* Navas Navarro, S. (2023). Robot Machines and Civil Liability. En *Algorithms and Law* (pp. 157-173), Cambridge University Press; Eidenmüller, H. (2021), The Rise of Robots and the Law of Humans. En *Law by Algorithm* (pp. 7-199). Mohr Siebeck, Tübingen; Wagner, G. (2023). Robot Liability. En *Algorithms and Law* (pp. 73-102). Cambridge University Press.

⁴² Sobre el particular, señala Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 4, que esta definición es «confusa», toda vez que «juntamente con los bienes muebles, la definición incluye determinados tipos de bienes que son intangibles». A este respecto, considera el autor citado que lo deseable sería que se contem-

entendiendo por tal «cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos», así como «la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos». A este concepto, hemos de anudar lo previsto en los apartados 2, 3 y 4 del mismo artículo sobre los archivos de fabricación digital, los servicios conexos y los componentes.

En este punto, no obstante, se plantean varias problemáticas relacionadas con el concepto que se incluye en la propuesta de Directiva y con determinados sujetos responsables (fundamentalmente, los programadores y los desarrolladores de los sistemas de inteligencia artificial). Todas ellas se pueden deducir, directa o indirectamente, de los Considerandos 13, 14, 15, 16, 17, 24 y 27 de la propuesta de Directiva sobre productos defectuosos. En primer lugar, como se ha señalado, la definición de producto incorpora, en contraposición al *hardware*, el *software* (con exclusión, eso sí, del código fuente al tratarse de pura información). Este extremo se hace ampliando su aplicación a otros activos intangibles como los programas informáticos (sistemas operativos, microprogramas, programas de ordenador, aplicaciones o sistemas de inteligencia artificial⁴³). De hecho, el propio Considerando 13 reconoce que, cada vez con más frecuencia, se encuentran en el mercado y desempeñan un papel muy relevante para la seguridad de los productos. Y ello, puede producirse, o bien como productos «autónomos» o bien como un «componente» al integrarse en otro producto.

Una vez aclarado que tal *software* (ya sea o no un sistema de inteligencia artificial) queda bajo el amparo de la propuesta de Directiva, su Considerando 14 añade una nueva premisa: cuando estos programas informáticos y de código abierto se desarrollen o suministren al margen de una actividad comercial, no resultará de aplicación esta norma (al margen de que tengan que cumplir con las obligaciones impuestas en la Ley de Inteligencia Artificial). Su fundamento radica, para la Unión Europea, en la necesidad de no obstaculizar la innovación o la investigación. Sobre el particular, cabe aludir, por ejemplo, a plataformas como GitHub, en la que los usuarios comparten *software* y códigos colaborativos (como arquitecturas de redes neuronales) que se emplean, entre otros, en el ámbito de la investigación y que permite, incluso, introducir modificaciones por terceros para mejorarlos (o así se entiende). Claro está que es posible que se realicen actos fraudulentos sin que, incluso, el imple-

planen, por un lado, los bienes muebles (con o sin incorporación de elementos digitales) y, por otro lado, los elementos digitales propiamente dichos (esto es, los contenidos y servicios digitales).

⁴³ La doctrina ya había puesto de relieve la problemática existente en relación con el concepto de producto y la introducción en el mismo de los sistemas de inteligencia artificial. Por todos, *vid.* Chagal-Federkorn, K.A. (2019). Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers. *Stanford Law & Policy Review*, 30(61), 61-114.

mentador tenga conocimiento y que se generen problemas de ciberseguridad (como ha ocurrido con la filtración del código fuente de Twitter por un usuario anónimo). En tales escenarios, es ciertamente complejo determinar el sujeto responsable y que ha de responder por el daño causado.

Al margen de las críticas que puedan efectuarse a esta opción legislativa⁴⁴, conviene destacar que la finalidad comercial debe interpretarse en un sentido amplio. Así, con buen criterio a nuestro parecer, no solamente estamos ante una actividad de este tipo cuando se lleve a cabo a cambio de un precio, sino que se incluyen aquellos supuestos en los que «los datos personales se utilicen de forma distinta a la de mejorar la seguridad, la compatibilidad o la interoperabilidad del programa informático». A este respecto, bien es sabido que los datos personales representan uno de los bienes más preciados y que, por supuesto, tienen un valor económico⁴⁵. De este modo, si la supuesta gratuidad del programa está encubriendo, en realidad, un uso ilegítimo de estos datos personales (en otras palabras, estos son la contraprestación exigida), se ventilará la responsabilidad con arreglo a la propuesta de Directiva.

Cuestiones distintas y que merecen una mención diferenciada, son los denominados contenidos y servicios digitales⁴⁶, así como los archivos de fabricación digital. En cuanto a los primeros, hemos de partir de las definiciones ofrecidas por el artículo 2 de la Directiva (UE) 2019/770 sobre lo que se entiende por contenido digital, servicio digital o bienes con elementos digitales.

⁴⁴ En contra, por ejemplo, *vid.* Izquierdo Grau, G. (2023). *Software y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de software o de sistemas de inteligencia artificial*. *IDP. Revista de Internet, Derecho y Política*, (38), 8-9.

⁴⁵ Sobre este extremo se manifiesta el Considerando 24 de la Directiva (UE) 2019/770, así como parte de la doctrina. En este sentido, entre otros, *vid.* Aparicio Vaquero, J.P. (2019). El valor económico de un derecho fundamental: la monetización de los datos personales. En *El Derecho de las TIC en Iberoamérica* (pp. 1027-1035). La Ley Uruguay; (2021). La tipificación del contrato de suministro de contenidos y servicios digitales: entre la propiedad intelectual y el derecho de consumo. *Revista de educación y derecho*, (24), 1-33. <https://doi.org/10.1344/REYD2021.24.36290>; Castillo Parrilla, J. A. (2021). Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD. *La Ley Mercantil*, (82), 1-20; Espín Alba, I. (2020). Contrato de suministro de contenidos y servicios digitales en la Directiva 2019/770/UE. Datos, consumidores y «prosumidores» en el Mercado Único Digital. *Revista de Derecho Privado*, (6), 3-38; Fuenteseca Degeneffe, C. (2018). Mercado Único Digital: algunos aspectos de la regulación del suministro de contenidos digitales. *Revista de Derecho Civil*, (2), 107-148; Cámara Lapuente, S. (2020). Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales. En E. Arroyo Amayuelas, S. Cámara Lapuente (Dirs.), *El derecho privado en el nuevo paradigma digital* (pp. 141-175). Marcial Pons.

⁴⁶ Sobre la dificultad para diferenciar entre ambos conceptos, *vid.* Mischau, L. (2022). The Concept of Digital Content and Digital Services in European Contract Law. *European Journal of Consumer and Market Law*, (1), 6-13.

Como se desprende de lo anterior, los servicios digitales se integran o interconectan con un producto de tal forma que su ausencia impediría a este último desempeñar alguna de sus funciones (y para la propuesta de Directiva son servicios conexos que pueden ser considerados componentes). Como ejemplo, prevé el Considerando 17 el caso del suministro continuo de datos de tráfico en un sistema de navegación, cuya importancia es crucial. Pues bien, en principio, a estos servicios se les aplica lo previsto en la referida Directiva (UE) 2019/770, así como, en el ámbito contractual de la compraventa de bienes, la Directiva (UE) 2019/771. En todo caso, señala la propuesta de Directiva sobre productos defectuosos que, dada la importancia que tienen en relación con la seguridad del producto, se ha de ampliar la responsabilidad objetiva a los servicios digitales.

Sea como fuere, la conclusión relativa a la ausencia de aplicación de la propuesta de Directiva tiene un matiz esencial vinculado a dos extremos: la externalización del servicio y el control del fabricante. Así las cosas, el fabricante del producto podrá ser declarado responsable con arreglo a la propuesta de Directiva cuando estén bajo su control, ya sea porque sean suministrados por él o los recomiende o influya de otro modo en su suministro por un tercero. En estos escenarios, consideramos que se puede aplicar la solidaridad en atención a lo dispuesto a la Exposición de Motivos que acompañaba a la propuesta inicial de Directiva que declaraba la complementariedad de los instrumentos normativos europeos (entre los que incluía, expresamente, la Directiva (UE) 2019/770 y la Directiva (UE) 2019/771) y a tenor de su artículo 2.4 b), de tal modo que:

- Si el servicio es prestado por un tercero, la responsabilidad de los prestadores de servicios digitales se resolverá en atención a la Directiva (UE) 2019/770 y la Directiva (UE) 2019/771 y normativas nacionales de transposición.
- Si el fabricante suministra los servicios o mantiene el control sobre los mismos, su responsabilidad se depurará de conformidad con la propuesta de Directiva sobre productos defectuosos y dicho servicio conexo tendrá la consideración de componente del producto. En este sentido, el ámbito de aplicación de la mencionada propuesta de Directiva con respecto a estos servicios digitales se define en función de su vinculación (incorporación) a un producto⁴⁷. No obstante,

⁴⁷ A este respecto, pone de relieve Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 4, que, teniendo en cuenta que la vigencia de la propuesta de Directiva se hace depender de la efectiva incorporación del *software* en un bien (mueble) tangible (de tal forma que sin ellos el producto no podría realizar sus funciones),

afirma la doctrina⁴⁸ que no se debe interpretar el concepto de componente «en clave de accesoriedad respecto del producto concebido como un todo, sino como un integrante de este que conforma el todo».

Por lo que respecta a los archivos de fabricación digital, el antes mencionado artículo 4.2 de la propuesta de Directiva señala que se identifican con «una versión digital o plantilla digital de un bien mueble, que contiene la información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas» (tales como impresoras 3D, por ejemplo). Estos archivos, así como la propia electricidad, también se consideran productos, como no podía ser de otra manera. Desde esta perspectiva, si continuamos con el caso de la impresora 3D, encontramos hasta cuatro sujetos potencialmente responsables: el fabricante del *hardware*, el programador o desarrollador del *software* de la misma, el programador o desarrollador del archivo de fabricación digital y, en su caso, el implementador (en el sentido de la Ley de Inteligencia Artificial). Parece que se excluyen, por tanto y a pesar de que podrían englobarse en la amplia definición del artículo 4.2 de la propuesta de Directiva, todos los activos existentes en el metaverso.

Sea como fuere, son evidentes las coincidencias entre estos archivos y los contenidos digitales, por lo que, ciertamente, parece que el legislador europeo está incorporando estos últimos en la propuesta de Directiva. Así, algunos autores⁴⁹ consideran que lo idóneo sería que se formulara la definición por remisión a la Directiva (UE) 2019/770.

Por último, interesa poner de relieve la creciente prevalencia en la interconexión de productos, así como la capacidad de aprendizaje de los mismos⁵⁰ y que, en consecuencia, permanecen bajo el control del fabricante

«para construir un sistema coherente y en armonía con las Directivas sobre la falta de conformidad de los bienes y de los contenidos o servicios digitales (es decir, las Directivas (UE) 2019/770 y 2019/771 [*twin directives*]), (...) sería deseable que, en lugar de referirse al *software*, se hiciera referencia a los servicios digitales y que estos se definieran por remisión a lo dispuesto en la Directiva (UE) 2019/770». En un sentido similar, *vid.* Wendehorst, C. y Duller, Y. (2021). *Safety and Liability Related Aspects of Software*. Comisión Europea. Dirección General de Redes de Comunicaciones.

⁴⁸ Vid. Izquierdo Grau, G. (2023). *Software y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de software o de sistemas de inteligencia artificial*. *IDP. Revista de Internet, Derecho y Política*, (38), 5.

⁴⁹ *Ibidem*.

⁵⁰ Señalan Fernández Llorca, D., Charisi, V., Hamon, R., Sánchez, I. y Gómez, E. (2023). *Liability Regimes in the Age of AI: a Use-Case Driven. Analysis of the Burden of Proof*. *Journal of Artificial Intelligence Research*, 76, 613-644 que las propias características inherentes a los sistemas de inteligencia artificial y que generan importantes riesgos, como la opacidad, la imprevisibilidad o sus capacidades propias de aprendizaje continuo, pueden generar dificultades considerables a la hora de para demostrar la causalidad.

más allá del momento en el que se introducen en el mercado. A este respecto, es importante que se formulen reglas de responsabilidad solidaria, en su caso, y que se tenga en cuenta en la evaluación sobre la seguridad cuándo el fabricante perderá el citado control. Además, cabe plantear supuestos de responsabilidad en relación con la posible introducción en un producto de un componente defectuoso de otro fabricante, que precisan, asimismo, de la solidaridad entre los fabricantes.

Íntimamente relacionado con lo anterior, se plantean algunas situaciones conflictivas. En este sentido, adquiere especial vigencia en este ámbito el término de «producto acabado⁵¹» para referir a aquel que se pone en el mercado a disposición del público en general, «sin que requiera ulteriores modificaciones y sin que las actualizaciones puedan alterar dicha configuración». Así, es probable que el fabricante se encargue tanto del *hardware* como del *software* o que este último se realice por un desarrollador. Lo importante, es que, en el momento de comercializarlo, ambos están agregados y forman parte de un todo común (*bundled products*). Desde esta perspectiva, como se verá, la propuesta de Directiva arbitra la aplicación de una responsabilidad solidaria entre ambos (*ex* artículo 12), con independencia de la vinculación (contractual o no) que exista entre ambos sujetos⁵².

Por otro lado, cuando el producto se introduce en el mercado sin el *software* y, posteriormente, se introduce por parte de un tercero o de la propia víctima. En estos supuestos y atendiendo a las peculiares circunstancias, podría considerarse que el productor ha perdido el control y que se trata de un producto nuevo, si se concluye que se ha alterado de forma sustancial en cuanto a su funcionalidad, seguridad e interoperabilidad. Desde esta perspectiva, parece razonable entender que el productor (si se quiere, inicial) no responderá de los daños causados, sino que lo hará el tercero (en aplicación de los artículos 8.4 y 11.1 g) de la propuesta de Directiva) o, en el caso de la víctima, deberá soportar todos o parte de los perjuicios (*vid.* artículo 13.2 de la propuesta de Directiva). Y es que, ese tercero será considerado productor, a los efectos de la propuesta de Directiva, siempre que el daño se deba únicamente a su actuación y no intervenga la defectuosidad del propio producto

⁵¹ Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 7-8.

⁵² En este sentido se pronuncia Navas Navarro, S. (2023). Robot Machines and Civil Liability. En *Algorithms and Law* (pp. 157-173), Cambridge University Press. Asimismo, Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 7, señala que, frente a la víctima, «imperla la concepción global del producto, independientemente de la relación contractual existente entre el *hardware manufacturer* y el *software manufacturer*».

(artículo 13.1 de la propuesta de Directiva), pues, como señalan algunos autores, se trata de un «bien reacondicionado»⁵³.

Sea como fuere, el problema se torna más complejo cuando nos encontramos ante un *software* o sistemas de inteligencia artificial de uso libre (*open source software*). Como se destacó anteriormente, la propuesta de Directiva, de forma expresa, excluye su aplicación en estos casos, siempre que no se obtenga ningún tipo de contraprestación a cambio. No obstante, algunos autores⁵⁴ que se manifiestan en contra de esta opción legislativa, consideran que el desarrollador ha de ser considerado un productor y, por tanto, reparar el perjuicio de conformidad con la propuesta de Directiva. Por lo demás, la exoneración de responsabilidad del *hardware manufacturer* dependerá de si ha comercializado o no el producto con dicho *software* o si, por el contrario, se ha añadido una vez este ha perdido el control. Asimismo, tráiganse a colación las reflexiones sobre la intervención de un tercero o de la propia víctima.

A continuación, conviene que nos refiramos a la defectuosidad de los productos que, como idea previa, se producirá cuando no cumpla con las normas de seguridad. Pues bien, el artículo 7 de la propuesta de Directiva sobre productos defectuosos destaca que se considerará un producto como defectuoso cuando no ofrezca la seguridad que el público en general tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión Europea o nacional, teniendo en cuenta todas las circunstancias, entre otras: la presentación y características del producto (incluidos su etiquetado, diseño, características técnicas, composición y envase, y las instrucciones de montaje, instalación, uso y mantenimiento), el uso y el efecto razonablemente previsible o la posibilidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio. Así las cosas, introduce elementos novedosos para reflejar la naturaleza cambiante de los productos en la era digital (interconexión, funciones de autoaprendizaje) y presenta una lista no exhaustiva a valorar por los tribunales. Desde nuestra perspectiva, estos conceptos son demasiado ambiguos e indeterminados y, quizás, se debería haber optado por aludir exclusivamente al incumplimiento de la legislación sobre seguridad. No obstante, este extremo debe ser completado con las presunciones y la carga de la prueba de las que nos ocuparemos a continuación.

⁵³ Vid. Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 8.

⁵⁴ *Ibidem*, pp. 8-9.

3.2.2. Régimen de responsabilidad civil y presunciones

Por lo que respecta a la responsabilidad civil, *strictu sensu*, estamos ante un criterio de imputación objetivo, esto es, que no atiende a la culpa del sujeto. Asimismo, se establece la solidaridad (artículo 12 propuesta Directiva sobre productos defectuosos) entre los operadores económicos que sean responsables de los mismos daños. Esta responsabilidad, además, no cabe limitarla o excluirla a través de pacto (que se entenderá, desde nuestra perspectiva, nulo de pleno derecho) o del Derecho nacional (artículo 15 propuesta Directiva sobre productos defectuosos), ni por la intervención de un tercero (*vid.* artículo 13.1 propuesta Directiva sobre productos defectuosos).

No obstante, sí se puede aplicar una reducción e, incluso, suprimirse la responsabilidad, como consecuencia de la culpa exclusiva de la víctima (o de una persona de la que sea responsable). Asimismo, es posible aplicar una exención de la responsabilidad en los escenarios previstos en el artículo 11 de la Propuesta Directiva sobre productos defectuosos⁵⁵. Entre otros: cuando el operador económico no ha introducido el producto en el mercado, ni lo ha puesto en servicio o comercializado, o cuando el defecto se deba a que el producto se ajusta a los requisitos legales.

En este punto, interesa destacar, por su relevancia, el artículo 9 de la Propuesta Directiva sobre productos defectuosos. Este precepto establece la obligatoriedad de que los estados miembros garanticen que los órganos jurisdicciones tengan potestad para ordenar, a petición del demandado y previa presentación de hechos y pruebas suficientes, la exhibición de las pruebas pertinentes de que disponga. En todo caso, tal y como se prevé, ha de limitarse a lo estrictamente necesario y ha de realizarse de forma proporcionada, toda vez que es posible que exista información confidencial, secretos comerciales e incluso otros derechos de propiedad industrial o intelectual. Desde esta perspectiva, el demandado podrá solicitar, en tales circunstancias, que se adopten medidas para preservar la confidencialidad. De hecho, consideramos que estas últimas pueden adoptarse de oficio por el juez. Como se tendrá ocasión de comprobar, al igual que ocurre con la defectuosidad, también la exhibición de pruebas tiene mucha importancia en la responsabilidad.

⁵⁵ Igualmente, dentro de los mencionados casos de exención, interesa hacer especial mención a la causa contemplada en la letra c) del anterior precepto que se ocupa de los supuestos en los que es probable o bien que el defecto no existiera al tiempo de introducir, poner en servicio o comercializar el producto; o bien que se produjera con posterioridad. Sin embargo, ello no obsta para que deba responder el fabricante cuando el defecto se deba a un servicio conexo, a un programa informático (incluidas las actualizaciones o mejoras) o a la falta de actualizaciones o mejoras necesarias para mantener la seguridad, siempre que estén bajo su control.

Como resulta de las reglas procesales ordinarias, la carga de la prueba corresponde, en principio, al demandante. Sea como fuere, el artículo 10 de la propuesta Directiva sobre productos defectuosos incorpora tres presunciones, todas ellas, *iuris tantum* (ex artículo 10.5 propuesta Directiva sobre productos defectuosos):

A) La presunción del carácter defectuoso del producto tiene lugar en tres escenarios: en primer lugar, cuando no se cumple, por parte del demandado, con la obligación de exhibir las pruebas a las que nos referimos anteriormente; en segundo lugar, cuando se demuestre que el producto no cumple con los requisitos obligatorios de seguridad establecidos en la normativa europea o nacional; y, en tercer lugar, cuando el demandante pruebe que el daño deriva de un mal funcionamiento evidente del producto durante un uso razonablemente previsible del mismo. De todos ellos, quizás el que más problemática puede generar, por ser más valorativo, es este último. A nuestro entender, esta circunstancia se ha de relacionar con casos en los que sea palmaria la relación directa entre el incorrecto funcionamiento y el perjuicio causado.

B) La presunción del nexo causal entre la defectuosidad y el daño se produce cuando se compruebe que el producto es defectuoso y el perjuicio aparezca como compatible, generalmente, con el anterior. En este punto, a la subjetividad anterior, se suma una nueva problemática. Nos referimos a la «comprobación» de la mencionada defectuosidad y si cabe englobar en ella también los casos en los que dicho carácter, en aplicación de la regla antes expuesta, es presumido. Desde nuestra perspectiva, el término comprobar es relativamente ambiguo y, en aplicación del principio *pro consumatore*, debe interpretarse en un sentido amplio y extensivo, de tal suerte que también se incluyan los supuestos de presunción del defecto.

C) La presunción del carácter defectuoso del producto, del nexo causal, o de ambos, opera cuando un órgano jurisdiccional nacional considere que el demandante se enfrenta «dificultades excesivas, en particular debido a la complejidad técnica o científica» y cuando el demandante demuestre que es probable que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso y el daño, o ambos. En todo caso, consideramos que la aplicación de esta previsión ha de llevarse con mucha cautela y su vigencia ha de ser excepcional. Repárese en que si no se contemplan limitaciones se estaría acabando con las reglas procesales de forma injustificada y peligrosa, con los efectos y consecuencias que se derivan. Así las cosas, con buen criterio, se prevé la posibilidad de que el demandado impugne la existencia de dichas dificultades excesivas o la probabilidad citada.

En cuanto a los daños indemnizables, se contempla la reparación de todo tipo de pérdidas materiales: muerte o lesiones corporales, incluidos los daños

para la salud psicológica comprobados médicamente (es decir, morales); daños o destrucción de cualquier propiedad (excepto el propio producto defectuoso, un producto dañado por un componente defectuoso de ese producto y las propiedades utilizadas exclusivamente con fines profesionales) y la destrucción o corrupción de datos que no se utilicen exclusivamente con fines profesionales.

En relación con la prescripción y caducidad, encontramos hasta tres plazos diferentes en función del tipo de perjuicio y de las circunstancias concurrentes. En este sentido, se establece un plazo general de prescripción de tres años, a contar desde que la persona tuvo conocimiento o debería haber tenido razonablemente conocimiento. Por su parte, se incorpora un segundo periodo de caducidad (que entendemos que no se podrá, por tanto, interrumpir) de diez años, de tal forma que opera como un lapso temporal máximo. En otras palabras, si no se ha tenido (o podido tener) conocimiento de los daños, del carácter defectuoso y de la identidad del operador económico en diez años, prescribirá la acción con independencia del plazo general de tres años. No obstante, como decíamos, también la clase de daño tiene relevancia en este sector. Y es que, es posible establecer una excepción a lo señalado anteriormente cuando la víctima no hubiere podido incoar un procedimiento en el plazo de diez años debido a la latencia de un daño corporal. En tal circunstancia, el plazo de prescripción será de veinticinco años.

3.3. LA PROPUESTA DE DIRECTIVA RELATIVA A LA ADAPTACIÓN DE LAS NORMAS DE RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL A LA INTELIGENCIA ARTIFICIAL Y LAS PRESUNCIONES

Del estudio realizado por la Comisión Europea se concluye que la mayoría de las normativas nacionales disponen de un régimen subjetivo de responsabilidad, pero se considera que pueden existir problemas para demostrar el daño, por lo que se busca aligerar la carga de la prueba. A este respecto, reconoce la Unión que el denominado efecto de «caja negra» puede «dificultar o hacer excesivamente costoso para las víctimas determinar cuál es la persona responsable y probar que se cumplen los requisitos para una demanda de responsabilidad civil admisible». Además, al adaptar las normas por los órganos jurisdiccionales es probable que existan diferencias, lo cual daría lugar a una evidente inseguridad jurídica. Por este motivo, se arbitra la intervención de la Unión Europea para, por un lado, evitar la fragmentación y, por otro, evitar que se produzca un descenso de inversión económica en este sector.

Pues bien, la primera cuestión que cabe advertir es que, tal y como ponen de manifiesto algunos autores⁵⁶, esta propuesta de Directiva, de ser aprobada, podría encajar «sin fricción en los sistemas de responsabilidad civil existentes, ya que reflejan un enfoque que no toca la definición de conceptos fundamentales como “culpa” o “daño”, dado que el significado de esos conceptos varía considerablemente en los Estados miembros». Compartiendo esta postura, consideramos que, quizás, sería adecuado que se incluyera una definición sobre los daños indemnizables por dos motivos. Por un lado, precisamente por la gran diversidad existente en los Estados miembros que bien podría vaciar de contenido, en algún supuesto, la posible indemnización al no contemplar determinados conceptos. Y, por otro lado, por las peculiaridades existentes en el sector que nos ocupa, tanto por la cuantía de los perjuicios como por la amplia tipología de daños.

Igualmente, es importante destacar que, al igual que en la propuesta de Directiva sobre productos defectuosos (*ex art.* 9), el artículo 3 de la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial establece el régimen de exhibición de pruebas. A este respecto, este precepto establece la obligatoriedad de que los Estados miembros garanticen que los órganos jurisdiccionales tengan potestad para ordenar, a petición del demandado y previa presentación de hechos y pruebas suficientes, la exhibición de las pruebas pertinentes de que disponga. En todo caso, tal y como se prevé, ha de limitarse a lo estrictamente necesario y ha de llevarse a cabo de forma proporcionada, toda vez que es posible que exista información confidencial, secretos comerciales e, incluso, otros derechos de propiedad industrial o intelectual. Desde esta perspectiva, el demandado podrá solicitar, en tales circunstancias, que se adopten medidas para preservar la confidencialidad. De hecho, estas últimas pueden adoptarse de oficio por el juez.

No obstante, acompaña a este extremo, atendiendo al propio tipo de responsabilidad (subjetiva) aplicable, de una presunción de culpabilidad en caso de incumplimiento (*vid.* Art. 3.5 de la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial). Sin embargo, esta regla general tiene matices en función del tipo de sistema y de la consideración del demandado. Es este sentido, cuando se trate de un sistema de alto riesgo, a la luz de las disposiciones relativas a la gestión de riesgos y sus resultados incorporados en la Ley de Inteligencia Artificial se considerará que existe culpa en cualquiera de los casos descritos en el artículo

⁵⁶ Fernández Hernández, C. (2022). La Comisión presenta una propuesta de Directiva sobre responsabilidad civil por daños causados por la IA (AI Liability Directive). *Derecho Digital e Innovación. Digital Law and Innovation Review*, (13), 1-7.

4.2 de la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial.

Sea como fuere, cuando estemos ante un sistema de alto riesgo no se presumirá la culpa si el demandante tiene la condición de usuario -«implementador», esto es, que su uso se enmarque en una actividad personal de carácter no profesional- y el demandado demuestre que no cumplió con sus obligaciones de utilizar o supervisar el sistema de conformidad con las instrucciones o que le expuso a datos de entrada que no eran pertinentes en atención a su finalidad.

A partir de aquí, el artículo 4 de la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, en una compleja redacción, incorpora una presunción general del nexo causal entre la culpa y el daño cuando: se haya probado la culpa por el demandante o se haya recurrido a la presunción de la negligencia descrita anteriormente; pueda considerarse razonablemente probable que la culpa ha influido en la producción del resultado (sin concretar, en todo caso, quién ha de probar esta probabilidad razonable y si se permite la apreciación, de oficio, por el tribunal); y el demandante haya probado que la información de salida (o su no producción) causó el daño. A pesar de que entendemos que estas herramientas han de examinarse con precaución y prudencia, la Comisión considera que puede resultar muy difícil probar la causalidad para los demandantes y que es la medida menos gravosa para dar respuesta a la necesidad de asegurar una indemnización justa para la víctima. Para parte de la doctrina científica⁵⁷ se contempla este extremo para tratar de alcanzar un equilibrio entre la protección de los perjudicados y el fomento de la innovación por parte del empresariado.

Esta dicotomía implica admitir, en palabras de la doctrina⁵⁸, que «en la estructura de las demandas por daños derivados de un sistema de IA por el que concurre culpa coexisten, con respecto a los mismos daños, dos nexos causales». Y, en realidad, responden a una misma finalidad: evitar que el efecto de «caja negra» desincentive a las víctimas a reclamar por el perjuicio sufrido en orden a las dificultades probatorias existentes y al elevado coste que conlleva.

En todo caso, de nuevo disponemos de «excepciones» en atención a la clase de sistema y al demandado. En este sentido, los apartados 4, 5 y 6 del artículo 4 de la propuesta de Directiva para la adaptación de las normas de

⁵⁷ Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret: Revista para el Análisis del Derecho*, (3), 72.

⁵⁸ Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 2.

responsabilidad civil extracontractual a la inteligencia artificial articulan una serie de medidas para paliar ciertos efectos injustos y que resumiremos a continuación:

- Sistemas de alto riesgo: no se presumirá el nexo cuando el demandado demuestre que el demandante podía acceder a pruebas y conocimientos especializados suficientes para probarlo.
- Sistemas que no sean de alto riesgo: solo se aplicará la presunción de la causalidad cuando el órgano jurisdiccional nacional considere excesivamente difícil para el demandante demostrarlo.
- Demandado desarrollando actividad personal (de carácter no profesional): solo se recurrirá a la presunción cuando el demandado haya interferido sustancialmente en las condiciones de funcionamiento del sistema o cuando tuviese la obligación y estuviese en condiciones de determinar sus condiciones de funcionamiento y no lo haya hecho.

Sobre el particular, parece deducirse que «mientras que en los procedimientos concernientes a los primeros la regla general será la aplicación de la presunción de causalidad, en los referentes a sistemas de IA que no sean de alto riesgo la misma pretensión solo resultará de aplicación excepcional, cuando los tribunales aprecien una excesiva dificultad para el actor de probar el nexo causal⁵⁹». Esta distinción, que no encuentra explicación en la propuesta de Directiva, no resulta adecuada para el autor citado, pues señala que existirán supuestos en los que, precisamente, sean los sistemas que no presentan alto riesgo los que generen un daño de más entidad. Siendo ello cierto, y a pesar de las excepciones que efectivamente pueden producirse en la práctica, entendemos que la evaluación de riesgos que fundamenta la propia clasificación entre los sistemas sustenta las anteriores diferencias en relación con la aplicación de presunciones. En otras palabras, desde un punto de vista estadístico, serán los sistemas de alto riesgo los que generen perjuicios con más frecuencia y con mayor incidencia en los derechos subjetivos, por su propia naturaleza.

Para la doctrina⁶⁰, dado que la Ley de Inteligencia Artificial, en estos casos, establece requisitos específicos de documentación, información y registro, pero no otorga al perjudicado el derecho a acceder a tal información, «el establecimiento de normas de exhibición cobra especial sentido, tanto por el hecho de que estará o, al menos deberá estar disponible, una información

⁵⁹ Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 3.

⁶⁰ Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret: Revista para el Análisis del Derecho*, (3), 72.

muy relevante para facilitar la prueba, como porque el deber de exhibición crea un incentivo adicional para cumplir los requisitos establecidos en la Ley de IA para documentar o registrar la información pertinente».

Además, afirma la doctrina⁶¹ que la Comisión ha escogido la herramienta menos intervencionista, al servirse de presunciones refutables (*rebuttable presumptions*) para aliviar la carga de la prueba. Se deduce, pues, que no se plantea una inversión del *onus probandi*, lo cual obstaculizaría la innovación de productos y servicios basados en inteligencia artificial.

Asimismo, con respecto al encaje del sistema de presunciones en el derecho de daños español, apunta algún autor⁶² que resulta coherente con el régimen subjetivo de responsabilidad del artículo 1902 CC y, al comentar el artículo 4.1 de la propuesta de Directiva, señala que la probabilidad razonable puede coincidir con el criterio de imputación objetiva de la causalidad adecuada. Sea como fuere, como quiera que el demandante debería probar el nexo de causalidad y que este extremo resultaría incoherente con la propuesta de Directiva (lo cual se pone de relieve, en especial, de los ejemplos incluidos en su Considerando 25), afirma el autor que esta última «simplifica al máximo la cuestión y parece apuntar a que la mera acreditación de la culpa del demandado, por sí sola, ya tiene que evidenciar la causalidad con respecto a la producción o no producción de información en el sistema de IA».

Sobre el particular, señalan algunos autores⁶³ que no se trata de permitir al juez utilizar un estándar de prueba reducido (causalidad probabilística), sino que le faculta para presumir el nexo causal entre la acción culposa y la información o falta de información del sistema, atendiendo a las circunstancias del caso concreto.

BIBLIOGRAFÍA

Aparicio Vaquero, J.P. (2019). El valor económico de un derecho fundamental: la monetización de los datos personales. En *El Derecho de las TIC en Iberoamérica* (pp. 1027-1035). La Ley Uruguay.

⁶¹ Fernández Hernández, C. (2022). La Comisión presenta una propuesta de Directiva sobre responsabilidad civil por daños causados por la IA (AI Liability Directive). *Derecho Digital e Innovación. Digital Law and Innovation Review*, (13), 1-7.

⁶² Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 3-4.

⁶³ Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret: Revista para el Análisis del Derecho*, (3), 72.

- (2021). La tipificación del contrato de suministro de contenidos y servicios digitales: entre la propiedad intelectual y el derecho de consumo. *Revista de educación y derecho*, (24), 1-33. <https://doi.org/10.1344/REYD2021.24.36290>
- Astray Chacón, M.P. (2023). Daños causados por la inteligencia artificial. *Actualidad Civil*, (7).
- Atienza Navarro, M. L. (2023). ¿Una nueva responsabilidad por productos defectuosos?, Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495). *InDret: Revista para el Análisis del Derecho*, (2), 1-53.
- BARRIO ANDRÉS, M. (2024). Algunos claroscuros en el Reglamento Europeo de Inteligencia Artificial. *Diario La Ley*, 86, 1-6.
- Cámara Lapuente, S. (2020). Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales. En E. Arroyo Amayuelas, S. Cámara Lapuente (Dirs.), *El derecho privado en el nuevo paradigma digital* (pp. 141-175). Marcial Pons.
- Castells i Marquès, M. (2019). Drones recreativos: normativa aplicable, responsabilidad civil y protección de datos. *Revista de Derecho Civil*, 6(1), 297-333.
- Castillo Parrilla, J. A. (2021). Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD. *La Ley Mercantil*, (82), 1-20.
- Čerka, P., Grigienė, J. y Širbikytė, G. (2015). Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, 31(3), 376-389.
- Chagal-Federkorn, K.A. (2019). Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers. *Stanford Law & Policy Review*, 30(61), 61-114.
- Churnin, S. (2011). *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*. Servicio de Publicaciones de la Facultad de Derecho. Universidad Complutense de Madrid.
- Cohen, I.G. (2020). Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?. *Georgetown Law Journal*, 108, 1425-1469.
- Cotino Hueso, L. (2024). La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial. *Diario LA LEY*, 80, 1-15.
- Eidenmüller, H. (2021), The Rise of Robots and the Law of Humans. En *Law by Algorithm* (pp. 7-199). Mohr Siebeck, Tübingen.
- Espín Alba, I. (2020). Contrato de suministro de contenidos y servicios digitales en la Directiva 2019/770/UE. Datos, consumidores y «prosumidores» en el Mercado Único Digital. *Revista de Derecho Privado*, (6), 3-38.
- Evans, B.J. y Pasquale, F. (2020). Product Liability Suits for FDA-Regulated AI/ML Software. *SSRN*, 1-15.

- Fernández Hernández, C. (2022). La Comisión presenta una propuesta de Directiva sobre responsabilidad civil por daños causados por la IA (AI Liability Directive). *Derecho Digital e Innovación. Digital Law and Innovation Review*, (13), 1-7.
- (2022). La Ley 15/2022 introduce la primera regulación positiva de la inteligencia artificial en España. *Diario La Ley*, (64), 1-8.
- Fernández Hernández, C., Eguiluz Castañeira, J.A. (2024). Diez puntos críticos del Reglamento europeo de Inteligencia Artificial. *Diario LA LEY*, 85, 1-38.
- Fernández Llorca, D., Charisi, V., Hamon, R., Sánchez, I. y Gómez, E. (2023). Liability Regimes in the Age of AI: a Use-Case Driven. Analysis of the Burden of Proof. *Journal of Artificial Intelligence Research*, 76, 613-644.
- Fuenteseca Degeneffe, C. (2018). Mercado Único Digital: algunos aspectos de la regulación del suministro de contenidos digitales. *Revista de Derecho Civil*, (2), 107-148.
- García-Prieto Cuesta, J. (2018). ¿Qué es un robot?. En *Derecho de los robots* (pp. 25-60). Wolters Kluwer.
- Garza-Ulloa, J. (2018). Chapter 6 - Application of mathematical models in biomechatronics: artificial intelligence and time-frequency analysis. En *Applied Biomechatronics using Mathematical Models* (pp. 373-524). Academic Press.
- Holme, D. (2017). Using artificial intelligence: not pie in the sky. *Practical Law UK Articles*, 1-3.
- Izquierdo Grau, G. (2023). *Software* y algoritmos defectuosos: algunas consideraciones sobre la responsabilidad del desarrollador de *software* o de sistemas de inteligencia artificial. *IDP. Revista de Internet, Derecho y Política*, (38), 1-12.
- Jaume-Palasi, L. (2020). Cómo la inteligencia artificial está impactando en las sociedades. En A. Cerrillo Martínez y M. Peguera Poch (Coords.), *Retos jurídicos de la inteligencia artificial* (pp. 27-39). Aranzadi.
- Kaul, V.; Enslin, S. y Gross, S.A. (2020). History of artificial intelligence in medicine. *Gastrointestinal Endoscopy*, 92(4), 807-812.
- Kemp, R. (2017). Artificial Intelligence: introduction. *Practical Law UK Articles*.
- Kulkarni, S., Seneviratne, N., Baig, M.S. y Ahmed Khan, A.H. (2020). Artificial Intelligence in medicine: where are we now?. *Academic Radiology*, 27(1), 62-70.
- Lacruz Mantecón, M.L. (2019). Cibernética y Derecho europeo: ¿una inteligencia robótica?. *Diario La Ley*, (9376), 1-19.
- (2020). *Robots y personas. Una aproximación jurídica a la subjetividad cibernética*. Reus.
- Martí Grau, R. (2023). Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños. *Revista Aranzadi Doctrinal*, (4), 1-9.
- Martín Casals, M. (2023). Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret: Revista para el Análisis del Derecho*, (3), 55-100.

- (2023). La regulación de la responsabilidad extracontractual por daños causados por sistemas de inteligencia artificial (IA) mediante dos propuestas de directiva. *Revista de responsabilidad civil, circulación y seguro*, (1), 6-30.
- Mathew, A., Amudha, P. y Sivakumari, S. (2020). Deep Learning Techniques: An Overview. En *Advances in Intelligent Systems and Computing* (pp. 599-608). Springer.
- McCarthy, J., et al. (1955). A proposal for the dartmouth summer research project on artificial intelligence. 1-13. Disponible en: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> (fecha última consulta: 01.07.2024).
- Mischau, L. (2022). The Concept of Digital Content and Digital Services in European Contract Law. *European Journal of Consumer and Market Law*, (1), 6-13.
- Monterroso Casado, E. (2010). Repercusiones de la inteligencia artificial en el ámbito de la responsabilidad civil. *Revista de responsabilidad civil, circulación y seguro*, (11), 6-20.
- Murphy, R.R. (2019). *Introduction to AI Robotics*. The MIT Press.
- Muñoz Vela, J. M. (2023). IA y responsabilidad civil. Comentarios a las propuestas europeas en materia de derechos de daños por productos defectuosos y adaptación de las normas de responsabilidad civil extracontractual. *Revista Aranzadi de derecho y nuevas tecnologías*, (61).
- Nappert, S. (2018). The challenge of artificial intelligence in arbitral decision-making. *Practical Law UK Articles*, 1-7.
- Navas Navarro, S. (Coord.). (2021). Salud electrónica e inteligencia artificial. En *Salud e inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid- 19)* (pp. 1-50). Comares.
- (2023). Robot Machines and Civil Liability. En *Algorithms and Law* (pp. 157-173), Cambridge University Press.
- Núñez Zorrilla, M.C. (2019). *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*. Reus.
- Ramón Fernández, F. (2019). Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?. *Diario La Ley*, (9365), 1-13.
- Reyes López, M.J. (2023). La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias. *Actualidad Civil*, (7).
- Rodríguez De Las Heras Ballell, T. (2023). La revisión de la Directiva de responsabilidad por producto: una pieza clave en el puzle de la responsabilidad por daños causados por inteligencia artificial. *LA LEY mercantil*, (103).
- Sanz de Galdeano, M. (2024). Neuroderechos: Todavía en las afueras del Derecho (A propósito de la comparecencia de Rafael Yuste en el Congreso). *Diario LA LEY*, (81), 1-5.
- Solar Cayón, J.I. (2019). *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*. Aranzadi.

- Torrubia Chalmeta, B. (2020). Aeronaves civiles no tripuladas. Contexto y regulación. En *Retos jurídicos de la inteligencia artificial* (pp. 255-267). Aranzadi.
- Turing, A. (1950). Computing Machinery and Intelligence. *Mind*, 59(236), 433-460.
- Tuset Varela, D. (2024). La regulación de la inteligencia artificial en Perú: liderando el desarrollo ético y responsable de la IA en América Latina. *Diario LA LEY*, (83), 1-13.
- Wagner, G. (2023). Robot Liability. En *Algorithms and Law* (pp. 73-102). Cambridge University Press.
- Wazid, M., Das, A.K., Chamola, V. y Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT express*, 8(3), 313-321.
- Wendehorst, C. y Duller, Y. (2021). Safety and Liability Related Aspects of Software. *Comisión Europea. Dirección General de Redes de Comunicaciones*.
- Zurita Martín, I. (2020). *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*. Reus.

Perspectiva y categorización del riesgo en el Reglamento de Inteligencia Artificial

MIQUEL PEGUERA

*Catedrático de Derecho mercantil
Universitat Oberta de Catalunya
mpeguera@uoc.edu*

Sumario: 1. INTRODUCCIÓN. 2. LA PERSPECTIVA DEL RIESGO. 3. LA PROHIBICIÓN DE PRÁCTICAS DE IA QUE IMPLICAN UN RIESGO EXCESIVO. 4. SISTEMAS DE IA DE ALTO RIESGO VINCULADOS A LA LEGISLACIÓN ARMONIZADA SOBRE SEGURIDAD DE PRODUCTOS. 5. SISTEMAS DE IA DE ALTO RIESGO INDEPENDIENTES. 5.1. Ejemplos de casos de uso relevantes. 5.2. Criterios para rechazar la calificación de riesgo alto. 5.3. Modificaciones de la relación de casos del Anexo III. 6. OBLIGACIONES DE TRANSPARENCIA FRENTE A RIESGOS DE CONFUSIÓN. 7. RIESGOS SISTÉMICOS DE LOS MODELOS DE USO GENERAL.

1. INTRODUCCIÓN

Aparentemente, la Unión Europea ha culminado con éxito, por lo menos en términos políticos, su audaz apuesta regulatoria en materia de IA con la aprobación del Reglamento de Inteligencia Artificial (en adelante, RIA), publicado en el Diario Oficial el 12 de julio de 2024.¹ Con una tramitación larga

¹ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DO L, 2024/1689, 12.7.2024.

y compleja -algo habitual en instrumentos de este calado-, el RIA ha salido adelante y ha establecido un marco legal que aspira abiertamente a provocar de nuevo un ‘efecto Bruselas’ que lo convierta en modelo a seguir en otras jurisdicciones,² como ya ocurrió con el Reglamento General de Protección de Datos (RGPD).³ Desde luego, éxitos pasados no garantizan éxitos futuros y nada asegura que el RIA vaya a lograr un reconocimiento similar. Entre otros motivos, porque en este caso el objeto de regulación difícilmente resiste una comparación con la protección de datos personales, un campo en el que la UE ya había acumulado una larga experiencia. Por una parte, experiencia legislativa, con diversas directivas, en especial la Directiva de 1995,⁴ y con la consagración del derecho de protección de datos como derecho distinto al de privacidad en la Carta Europea de Derechos Fundamentales. Y por otra parte, también experiencia de aplicación judicial, con relevantes pronunciamientos del Tribunal de Justicia de la UE; así como experiencia de aplicación por las autoridades de protección de datos, junto con la reflexión, orientaciones y dictámenes del Grupo del Art. 29.⁵ Todos estos precedentes hicieron posible alumbrar en 2016 una norma como el RGPD, que si bien ha alcanzado un notable predicamento global, suscita también críticas y no faltan voces que urgen a su reforma.

Ese caudal de experiencia regulatoria y de aplicación que acompañó la gestación del RGPD está ausente en el caso de la inteligencia artificial. Más aún: tratándose establecer un marco jurídico para la IA, el propio objeto de regulación resulta movedizo y de difícil aprehensión, a pesar de los intentos de definición. Con un objeto por naturaleza disruptivo y de contornos cambiantes, el legislador se enfrenta a un reto mayúsculo y bien se le puede aplicar la metáfora de la justicia ciega: aquí no en el sentido de aplicar el Derecho sin prejuicios, sino en el sentido de legislar con los ojos vendados por la imposibilidad de avizorar cabalmente las características del fenómeno que se dispone a regular, o por lo menos, los rasgos que este fenómeno puede presentar en el futuro más inmediato, por no hablar ya de los que puede revestir a medio plazo.

² Así, el Consejo Europeo se fijó como objetivo que la UE “sea un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética”. Vid. Consejo Europeo, *Conclusiones de la Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020)*, EUCO 13/20, 2020, p. 6.

³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1-88.

⁴ La hoy derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31-50.

⁵ Hoy Comité Europeo de Protección de Datos (cfr. art. 68 del RGPD).

En estas condiciones, el riesgo de obsolescencia normativa es muy elevado. Ello explica que el RIA contenga numerosas remisiones a futuros desarrollos y concreciones que se confían a la Comisión Europea, a las entidades clave en la estructura de gobernanza que dibuja el propio Reglamento, así como a los organismos europeos de normalización que van a tener un papel fundamental en la traducción a estándares los requisitos previstos en el RIA.

Una muestra ilustrativa del carácter ineludiblemente provisional del enfoque regulatorio se puso de manifiesto en la necesidad de reaccionar con urgencia ante tras el lanzamiento de ChatGPT en noviembre de 2022, que hizo evidente el papel de los grandes modelos de lenguaje (LLM), aptos para múltiples propósitos prácticos. Se trataba de algo que el texto del Reglamento propuesto por la Comisión poco más de un año y medio antes, en abril de 2021, no había sido capaz de anticipar, de modo que tanto el Consejo como el Parlamento se apresuraron a formular enmiendas para acoger modelos y sistemas de propósito general, frente al esquema inicial de la propuesta, que se centraba en sistemas previstos para finalidades específicas.

Todo ello no significa que el RIA haya surgido de la nada. Estuvo ciertamente precedido por múltiples estudios y trabajos. Pero siempre en un marco de incertidumbre sobre el modo en que el legislador debía actuar ante el imparable desarrollo de las tecnologías de IA. En un escenario así, regular comporta el riesgo de llegar *demasiado pronto* y comprometer con trabas legislativas el desarrollo de la IA, la innovación y la efectiva adopción de sistemas de IA en la UE. A la vez, la eventual decisión de diferir la intervención legislativa a la espera de comprobar cómo se desarrolla este fenómeno implica el riesgo de llegar *demasiado tarde*, cuando quizás ya no es posible reconducir algunos de los efectos negativos consolidados.

En este contexto, el legislador ha adoptado en el Reglamento varias decisiones clave. Una de ellas es la de enfocar la regulación desde la lógica de la seguridad de productos, un campo en el que la UE goza ciertamente de una larga experiencia, pero cuya aptitud para abordar el complejo fenómeno de la IA no resulta evidente.

Otra de las decisiones esenciales de política jurídica ha consistido en construir un régimen jurídico enfocado a eliminar o mitigar los potenciales riesgos del empleo de sistemas de IA. Esta óptica del riesgo -de los peligros que los sistemas de IA pueden representar para la salud, la seguridad y los derechos consagrados en la Carta Europea de Derechos Fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente en la Unión Europea-⁶ permite al legislador sostener que la intervención normati-

⁶ Cfr. Art. 1 RIA.

va se limita a ofrecer salvaguardas frente los riesgos más graves -en ocasiones llegando a la prohibición total de ciertas prácticas de IA-, sin ir más allá de lo estrictamente necesario para este propósito y dejando un amplio margen de libertad para el desarrollo, comercialización y utilización de sistemas que no comporten tales peligros.

La lectura del RIA desde la óptica del riesgo permite interpretarlo como un texto que establece diversos conjuntos de requisitos y obligaciones en atención al nivel de riesgo que plantea la introducción en el comercio, puesta en servicio y utilización de sistemas de IA, y que varían en función de sus capacidades, finalidad, y ámbito en el que se emplean. Aunque no se trata de una perfecta gradación, distinguimos fácilmente entre un grupo de usos o prácticas de IA que se declaran prohibidas, por revestir un nivel de riesgo potencial excesivo o inaceptable, y un grupo de supuestos de riesgo alto, al que se destinan la mayor parte de las previsiones del texto. Por otra parte, se fijan obligaciones para los llamados modelos de uso general, con obligaciones particulares en los casos en que estos modelos plantean riesgos sistémicos. Finalmente, se identifican ciertos sistemas que por sus características particulares -la confusión o desinformación que pueden provocar a personas que desconocen que se hallan ante actividades desarrolladas, o contenidos generados, por IA- quedan sujetos a ciertas obligaciones de transparencia e información. En rigor, no se trata de sistemas de “riesgo limitado”, ya que estos mismos sistemas pueden ser, a su vez, sistemas de alto riesgo, en cuyo caso deberán cumplir los correspondientes requisitos de modo cumulativo.

La delimitación del catálogo de prácticas prohibidas, y de aquellas que se consideran de alto riesgo y sujetas por tanto a un gravoso conjunto de exigencias regulatorias, es un punto de partida que adopta el legislador confiando en algunos estudios y análisis preliminares. Esta clasificación, sin embargo, no parece completamente ajena a ciertos apriorismos, ni a las influencias ejercidas por la industria y por el activismo civil y está llamada a sufrir modificaciones. A su vez, el propio RIA arbitra la posibilidad de que, en el caso concreto, un sistema subsumible en la relación ámbitos y casos de alto riesgo, pueda escapar a esta calificación si resulta suficientemente justificado, a partir de determinados criterios, que el nivel de riesgo que plantea es de carácter menor.

2. LA PERSPECTIVA DEL RIESGO

El *iter* legislativo del RIA se inicia formalmente con la publicación de la Propuesta de Reglamento por parte de la Comisión, el 21 de abril de

2021,⁷ que viene a recoger la estela de los trabajos previos. Así, en abril de 2018, la Comisión publicó su comunicación *Inteligencia artificial para Europa*.⁸ En diciembre del mismo año, preparó un *Plan coordinado sobre la inteligencia artificial*,⁹ y en abril de 2019, hizo pública una nueva comunicación, titulada *Generar confianza en la inteligencia artificial centrada en el ser humano*.¹⁰ También en 2019, el Grupo de expertos de alto nivel sobre IA, nombrado por la Comisión el año anterior, elaboró unas *Directrices éticas para una IA fiable*.¹¹ Poco más tarde, la Comisión elaboró el *Libro Blanco sobre la inteligencia artificial*, publicado en febrero de 2020.¹² Por su parte, el Parlamento Europeo dictó una Resolución en octubre de 2020 sobre aspectos éticos de la IA, que recomendaba a la Comisión presentar una propuesta de instrumento legislativo para la regulación de la IA, incluyendo una detallada propuesta de texto articulado.¹³ Estos trabajos condujeron a la publicación de la propuesta de Reglamento de abril de 2021, que vino acompañada por los habituales documentos de evaluación del impacto de la misma.¹⁴

La justificación que se aportó para la intervención legislativa se refiere esencialmente a los problemas relacionados con el uso de los sistemas de IA y con las consecuencias de la ausencia de normativa armonizada en la materia. Tales problemas son, de un lado, los riesgos que se derivan del uso de la IA, particularmente en términos de salud, seguridad, y derechos fundamentales y valores de la UE. Por otra parte, la falta de seguridad jurídica en un campo no regulado y no armonizado. Esta falta de regulación lleva a una falta de confianza en la IA que perjudica el desarrollo de esta tecnología en Europa y reduce la competitividad de la UE. Esto exige una intervención al nivel de la

⁷ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021, COM(2021) 206 final.

⁸ Bruselas, 25.4.2018, COM(2018) 237 final.

⁹ Bruselas, 7.12.2018, COM(2018) 795 final.

¹⁰ Bruselas, 8.4.2019, COM(2019) 168 final.

¹¹ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, *Directrices éticas para una IA fiable*, Oficina de Publicaciones, 2019, <https://data.europa.eu/doi/10.2759/14078>.

¹² Comisión Europea, *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final.

¹³ Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html.

¹⁴ *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final.

UE, ya que las medidas que pudieran adoptar aisladamente los Estados miembros comportarían una indeseable fragmentación del mercado.¹⁵

En lo referido concretamente a la seguridad de productos, el marco legal en vigor se halla integrado por normas de carácter transversal, como el Reglamento (UE) 2023/988 de 10 de mayo de 2023 relativo a la seguridad general de los productos,¹⁶ que sustituye a la Directiva anterior; o el Reglamento 2019/1020 de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos.¹⁷ Se integra también por disposiciones sectoriales, como la Directiva sobre las Máquinas,¹⁸ que a partir del 20 de enero de 2027 quedará sustituida por el nuevo Reglamento relativo a las máquinas;¹⁹ el Reglamento sobre productos sanitarios;²⁰ o el Reglamento de seguridad de vehículos.²¹

Este marco normativo sobre seguridad resulta insuficiente para abordar los riesgos asociados al uso de la IA en productos. Por una parte, los riesgos que suscitan los productos físicos son distintos de los que plantea la IA: por

¹⁵ Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Brussels, 21.4.2021 SWD(2021) 84 final (Part 2), pp. 13-30.

¹⁶ Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo, DO L 135 de 23.5.2023, p. 1-51.

¹⁷ Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011, DOUE L 169, 25.6.2019, p. 1-44.

¹⁸ Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (refundición) DOUE L 157, 9.6.2006, p. 24-86, modificada en diversas ocasiones.

¹⁹ Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo, DO L 165 de 29.6.2023, p. 1-102.

²⁰ Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo, DOUE L 117, 5.5.2017, p. 1-175, varias veces modificado.

²¹ Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) 78/2009; (CE) 79/2009; y (CE) 661/2009 del Parlamento Europeo y del Consejo; y los diversos Reglamentos de la Comisión, DOUE L 325, 16.12.2019, p. 1-40, con diversas modificaciones ulteriores.

ejemplo, peligros vinculados a los sesgos presentes en los datos utilizados para entrenar modelos o diseñar algoritmos; problemas relacionados con la interpretación errónea de información en situaciones complejas; o efectos negativos que pueden repercutir en personas y bienes. Además, los riesgos pueden verse agravados por ataques externos que alteren los datos de entrada, a menudo de manera imperceptible, provocando fallos en el sistema. Por otra parte, la normativa vigente tampoco es adecuada porque, aunque cubre los riesgos derivados del software que actúa como componente de seguridad en productos, no contempla, más que en escasas excepciones, el software en sí mismo, ya sea el utilizado en servicios o el que se incorpore al producto tras su comercialización. Y en los supuestos en que el software sí está regulado, no se imponen requisitos suficientes para afrontar los riesgos propios de un sistema de IA, ni se considera la evolución continua de estos sistemas a lo largo del tiempo.²²

La constatación de los problemas apuntados y de las insuficiencias de la legislación vigente, junto con la consideración de diversas opciones de política jurídica, llevaron a la Comisión a proponer un Reglamento de alcance horizontal, teniendo en cuenta el nivel de riesgo que puede plantear el uso de la IA en diversos contextos.

Tanto el *Libro Blanco sobre la inteligencia artificial*²³ como las recomendaciones del Parlamento Europeo,²⁴ ambos ya citados, sugirieron adoptar un enfoque basado en el riesgo, con el objetivo de limitar la regulación a los casos de uso de la IA en los que la salud, la seguridad y los derechos fundamentales de los ciudadanos puedan verse más gravemente amenazados. En particular, en el Libro Blanco la Comisión consideró necesario seguir un enfoque basado en el riesgo para alcanzar un equilibrio que evite una carga desproporcionada a los actores implicados, en especial a las pymes. Esto requiere, como reconocía la Comisión, disponer de criterios claros para distinguir entre distintas aplicaciones de IA y determinar si entrañan o no un riesgo alto. A este propósito, sugirió que una aplicación de IA debería considerarse de alto riesgo cuando concurran cumulativamente los dos criterios siguientes. Por una parte, que se emplee en un *sector* en el que, por sus características o por las

²² Sobre esta percepción de la insuficiencia de la normativa de seguridad de productos, véase el *Impact Assessment* que acompaña la propuesta: *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final (Part 2), pp. 13-16.

²³ Comisión Europea: *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final.

²⁴ *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html.

actividades que normalmente se llevan a cabo, resulte previsible la existencia de riesgos significativos. Por otra parte, que, además de emplearse en uno de los sectores identificados, el *uso concreto* del sistema de IA pueda dar lugar a riesgos elevados.²⁵ En sentido similar, el Parlamento Europeo recomendó un enfoque basado en el riesgo y orientado al futuro, con normas transversales para todos los sectores y normas sectoriales cuando sea preciso. Al igual que el Libro Blanco, indicó que sería necesaria una lista exhaustiva y cumulativa de sectores de alto riesgo y de usos o fines de alto riesgo. Y que debería someterse a reevaluación periódica tanto la lista como la propia metodología de evaluación de riesgos.²⁶

Con algunas variaciones, este enfoque centrado en el riesgo es el que adoptó la propuesta y pasó al texto del RIA finalmente aprobado. En los siguientes epígrafes examinamos sumariamente la calificación de los riesgos que lleva al RIA a fijar prohibiciones absolutas para determinadas prácticas y a establecer un régimen particular para los sistemas de alto riesgo, tanto los que se enmarcan en la normativa armonizada de seguridad de productos como los sistemas independientes; a establecer ciertas obligaciones de transparencia en relación con determinados sistemas, destinadas a minimizar riesgos específicos, así como a fijar requisitos particulares para los modelos de uso general que presentan riesgo sistémico.

3. LA PROHIBICIÓN DE PRÁCTICAS DE IA QUE IMPLICAN UN RIESGO EXCESIVO

El listado de prácticas prohibidas, fijado en el artículo 5 del RIA, experimentó notables cambios a lo largo de la tramitación legislativa, llegando finalmente a una relación más extensa de la contemplada en la propuesta inicial, y con un detallado conjunto de matices y excepciones, particularmente en relación con determinados usos de la IA por los poderes públicos en materia de seguridad.

Un primer grupo de prácticas prohibidas se refiere a usos manipulativos o engañosos y de explotación y control social, que se prohíben por resultar esencialmente contrarias a los valores de la UE y a los derechos fundamentales reconocidos en la Carta. Se trata, por una parte, de los sistemas que empleen

²⁵ Véase el *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final, pp. 21-22.

²⁶ Véase *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))*, puntos 12 a 16.

técnicas subliminales que trasciendan la conciencia de una persona, o de técnicas deliberadamente manipuladoras o engañosas que persigan o produzcan el efecto de modificar sustancialmente el comportamiento de una persona o de un colectivo. Se requiere que tales técnicas mermen apreciablemente la capacidad para tomar una decisión informada e induzcan a tomar una decisión que de otro modo no habrían tomado. Además, se exige que con ello se provoque a esa persona o a otra, o a un colectivo, prejuicios considerables, o que, por lo menos, sea razonablemente probable ese resultado perjudicial.²⁷ En sentido similar, se prohíben los sistemas de IA que exploten alguna vulnerabilidad de una persona física o de un colectivo, que derivada de su edad, discapacidad o situación social o económica. De igual modo que en el caso anterior, el uso del sistema debe tener por objeto o por efecto alterar sustancialmente el comportamiento de la persona o personas afectadas, así como provocar perjuicios considerables a esa o a otra persona, o que tal perjuicio resulte razonablemente probable.²⁸

En ambos casos, la prohibición se refiere a la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA de tales características. Resulta notable el cúmulo de requisitos que exige el RIA para prohibir estas prácticas, lo que reduce el alcance de la prohibición, además de plantear dificultades interpretativas. En sus considerandos, el RIA advierte que las técnicas de manipulación, sea subliminal o de otro tipo, menoscaban la autonomía personal sin que la persona afectada sea consciente de ello, y que incluso cuando es consciente de que se están empleando estas técnicas, la persona afectada puede seguir siendo engañada o no puede controlarlas u oponer resistencia.

Tendría sentido que el empleo de tales técnicas resultara ya prohibido con carácter general, pero el Reglamento exige además el resultado del daño, o su probabilidad razonable, tanto en el caso de manipulación como en el de explotación de vulnerabilidades. Daño o perjuicio que puede ser de todo tipo, al haberse prescindido en el texto final de la caracterización establecida en la propuesta inicial, que exigía perjuicio de carácter físico o psicológico.

El alcance de ambas prohibiciones queda en cierto modo matizado por las indicaciones del considerando 29. En este se advierte que «no es necesario que el proveedor o el responsable del despliegue tengan la intención de causar un perjuicio considerable, siempre que dicho perjuicio se derive de las prácticas de manipulación o explotación que posibilita la IA». Al mismo tiempo se advierte que no puede presuponerse que existe la intención de alterar el comportamiento si tal alteración resulta de factores externos al sistema de IA, que ni el provee-

²⁷ Art. 5.1.a) RIA.

²⁸ Art. 5.1.b) RIA.

dor ni el responsable del despliegue controlan ni están en condiciones de mitigar -aunque conviene recordar que conforme al tenor del art. 5, en ninguno de los casos es necesaria tal intención sino que basta con que el sistema produzca el efecto de la alteración sustancial del comportamiento-. En sentido similar se advierte de que las prácticas comerciales comunes y legítimas, por ejemplo en el campo de la publicidad, que cumplan con el ordenamiento en vigor, no deben considerarse en sí mismas prácticas de manipulación perjudiciales. A este respecto, las conductas recogidas en estas prohibiciones ya estaban parcialmente contempladas, aunque no referidas de modo concreto a la IA, en la regulación sobre prácticas comerciales desleales.²⁹

El RIA opta también por prohibir de la introducción en el comercio, puesta en servicio o utilización de ciertos sistemas de IA de *social scoring* o “puntuación ciudadana”. En particular, se prohíben aquellos que se destinan a evaluar o clasificar a personas físicas o colectivos a lo largo de un cierto tiempo a partir de su comportamiento social o de “características personales o de su personalidad conocidas, inferidas o predichas”, y siempre que la puntuación resultante provoque alguna de las situaciones que contempla el precepto. Se trata específicamente de que ocasione un trato perjudicial o desfavorable “en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente”; o bien un trato perjudicial o desfavorable para las personas afectadas, “que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este”. Del tenor del precepto cabría colegir que si el trato perjudicial, o incluso meramente desfavorable, se produce en el mismo contexto en el que se recabaron los datos -por ejemplo el lugar de trabajo- el sistema no quedaría afectado por la prohibición, salvo que el trato resulte a su vez injustificado o desproporcionado. Por otra parte, no se proporcionan elementos para valorar el carácter injustificado o desproporcionado, a la vez que se da a entender que ese perjuicio podría resultar aceptable si guarda proporción con el comportamiento social observado, cuestión que suscita algunos interrogantes.

²⁹ En este sentido, el considerando 29 RIA expone que la prohibición complementa lo dispuesto en la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior (DOUE L 149, 11.6.2005). Como apuntaron VEALE y BORGESIUUS en relación con la propuesta de reglamento, la prohibición de este tipo de conductas de manipulación se estaba ya prevista el artículo 5 de la Directiva 2005/29/CE que considera desleal la práctica contraria a los requisitos de la diligencia profesional que “distorsiona o puede distorsionar de manera sustancial, con respecto al producto de que se trate, el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica, o del miembro medio del grupo, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores”, grupo que puede caracterizarse por ser consumidores especialmente vulnerables por padecer una dolencia física o un trastorno mental o por su edad o su credulidad. Vid. Michael VEALE, Frederik BORGESIUUS, “Demystifying the Draft EU Artificial Intelligence Act”, *Computer Law Review International* (2021) 22(4) 97-112, esp. p. 99.

El supuesto -como ocurre con muchos otros- plantea la dificultad de fijar las fronteras de la práctica prohibida. A diferencia de los casos de manipulación o de explotación de vulnerabilidades, aquí no se hace referencia a la aptitud en abstracto para provocar un prejuicio (probabilidad razonable), sino que incluye como parte de la definición del sistema cuyo uso se busca prohibir el hecho de que este provoque efectivamente el trato perjudicial o desfavorable antes mencionado. Tratándose de una circunstancia que sólo cabe apreciar *a posteriori*, la delimitación de la conducta prohibida parece poco afortunada y por tanto de escasa seguridad jurídica. No ayudan a una mejor precisión las observaciones del considerando 31, que señala que “deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación y *den lugar a* esos resultados perjudiciales o desfavorables”, y que a su vez advierte que la prohibición “no debe afectar a prácticas lícitas de evaluación de las personas físicas que se efectúen para un fin específico de conformidad con el Derecho de la Unión y nacional”.³⁰

Se consideran también sistemas de IA de riesgo excesivo, y en consecuencia se prohíbe su introducción en el mercado, su puesta en servicio para este fin y su uso, los destinados a predecir el riesgo de que una persona cometa un delito a partir únicamente de su perfil o de la evaluación de su personalidad,³¹ un supuesto no previsto en la propuesta inicial y que se acabó de concretar durante la negociación interinstitucional en los trílogos.³² La prohibición se fundamenta en la presunción de inocencia, en virtud de la cual las personas deben ser juzgadas basándose en su comportamiento real y no a partir de predicciones realizadas por un sistema de IA de estas características.³³ La prohibición alcanza sólo a predicciones basadas únicamente en la elaboración de perfiles o en la evaluación de los rasgos y características de la personalidad. Esto parece apuntar al hecho de que no haya habido una valoración humana, y así lo viene a sugerir el considerando 42. Aunque no se hace explícito en la norma, parece claro que se tienen en cuenta los riesgos discriminatorios de este tipo de sistemas predictivos, que pueden perjudicar a determinados individuos a consecuencia de los sesgos de los datos de entrenamiento.

Se excluyen expresamente de la prohibición los sistemas de IA utilizados para apoyar la valoración humana sobre la participación de una persona en una actividad delictiva, con base en hechos objetivos y verificables.³⁴ De acuer-

³⁰ Cdo. 31 RIA.

³¹ Art. 5.1.d) RIA.

³² Cabe notar, por otra parte, que la redacción final no incluye la predicción de incurrir o reincidir en infracciones administrativas, que había sido contemplada en las enmiendas del Parlamento de 14 de junio de 2023.

³³ Cdo. 42 RIA.

³⁴ Art. 5.1.d) RIA.

do con el considerando 42, esta prohibición no alcanza a los análisis de riesgos «que *no estén basados* en la elaboración de perfiles de personas o en los rasgos y características de la personalidad de las personas», y apunta como ejemplos el caso de los sistemas que evalúan la probabilidad de fraude financiero por parte de empresas a partir de transacciones sospechosas, o la probabilidad de localización de mercancías ilícitas por parte de autoridades aduaneras.³⁵

El reconocimiento facial ha sido un punto controvertido en la tramitación del Reglamento y finalmente se ha incluido una prohibición general de los sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción indiscriminada de imágenes de internet o de circuitos cerrados de televisión como las cámaras de seguridad. El fundamento alegado en este caso es la contribución de estos sistemas al agravamiento de la sensación de vigilancia masiva, y a su impacto en los derechos fundamentales, particularmente en el derecho a la intimidad.³⁶

Particularmente novedosa resulta la prohibición de sistemas de IA para inferir emociones en el lugar de trabajo o en centros educativos.³⁷ Diversas organizaciones habían solicitado una prohibición absoluta de estos sistemas, que finalmente se limitó a su uso en el ámbito de las relaciones de trabajo y en el campo de la educación, y contó con la pública oposición de parte de la industria, alegando los efectos beneficiosos que pueden reportar estas tecnologías. El fundamento expresado para esta prohibición se sitúa en las dudas que generan la fiabilidad y la base científica para la detección o deducción de emociones, que se manifiestan de modo diverso en distintas culturas y colectivos y que pueden conducir a resultados discriminatorios. El motivo para confinar la prohibición al ámbito laboral y educativo radica en que en estos contextos se da un desequilibrio de poder, que viene a añadirse al carácter intrusivo de estos sistemas. Se excluyen del ámbito de la prohibición aquellos sistemas que tengan fines exclusivamente médicos o de seguridad, lo que no parece referirse a la exclusión de sistemas de detección de dolor o cansancio a fin de evitar accidentes, pues el considerando 18 ya excluye estos objetivos de la propia noción de reconocimiento de emociones.³⁸

³⁵ Cdo. 42 RIA.

³⁶ Art. 5.1.d) RIA y Cdo. 43 RIA.

³⁷ Art. 5.1.f). Por “sistema de reconocimiento de emociones” se entiende, a efectos del Reglamento, «un sistema de IA destinado a distinguir o inferir las emociones o las *intenciones* de las personas físicas a partir de sus datos biométricos», vid. Art. 3.39) RIA.

³⁸ En efecto, el Considerando 18 precisa que «[e]l concepto [de reconocimiento de emociones] se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se

Por último, la biometría se halla en el centro de otros dos grupos de prohibiciones. Por una parte, se prohíben los sistemas que clasifican individualmente a las personas por sus datos biométricos para deducir o inferir datos sensibles como la raza, preferencias políticas o sindicales, convicciones religiosas o filosóficas, o la vida y orientación sexual. El precepto advierte que «esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho», lo que plantea de nuevo la cuestión de las fronteras del supuesto de hecho al que se aplica la prohibición. Por otra parte, se prohíben los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley (*law enforcement*), con una serie de excepciones. Se trata de un punto objeto de controversia y grandes esfuerzos de negociación, por el interés de los Estados en disponer de herramientas de este tipo para su actividad de control y cumplimiento de la ley. La norma recoge tres excepciones, que se refieren a los casos en que el uso de esta tecnología resulte estrictamente necesario para la búsqueda selectiva de víctimas de ciertos delitos y de personas desaparecidas; para prevenir amenazas inminentes contra la vida o seguridad y de amenazas reales y o previsibles de atentado terrorista; o para localizar o identificar a un sospechoso de determinados delitos, recogidos en el Anexo II del Reglamento.³⁹

4. SISTEMAS DE IA DE ALTO RIESGO VINCULADOS A LA LEGISLACIÓN ARMONIZADA SOBRE SEGURIDAD DE PRODUCTOS

Como señalamos en la introducción, junto con la decisión de adoptar una perspectiva que atiende al riesgo, el legislador europeo tomó también la decisión de insertar la regulación, en la medida de lo posible, en el marco de la normativa de seguridad de productos, considerando que muchas de las soluciones de IA van a estar vinculadas a productos para los que ya existe regulación sectorial de seguridad. En este sentido, el RIA busca aprovechar este bloque de normativa armonizada para encajar en ella los nuevos requisitos que se van a requerir a los sistemas de IA vinculados a los productos cubiertos por dicha legislación.

utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro».

³⁹ Las excepciones a esta prohibición se rodean de precisas cautelas y salvaguardas que el RIA prevé en los apartados 2 a 7 del artículo 5.

Ese conjunto de normas de seguridad de productos se divide en dos grupos, según se trate de disposiciones dictadas conforme al llamado “nuevo marco legislativo para la comercialización de productos”,⁴⁰ establecido en 2008, o bien se trate de normas armonizadas anteriores. Entre las dictadas al amparo del nuevo marco legislativo se incluyen, entre otras, normas referidas a juguetes, máquinas, embarcaciones, ascensores, equipos radioeléctricos, equipos a presión o productos sanitarios. Entre las normas anteriores se hallan disposiciones sobre vehículos de motor, aviación civil, equipos marinos o sistema ferroviario, entre otros.⁴¹

En el contexto de esta legislación armonizada de seguridad de producto, y más específicamente en el marco del listado de disposiciones concretas de esa legislación que recoge el Anexo I, el RIA considera que son sistemas de AI de alto riesgo aquellos que constituyan, en sí mismos, un producto de los contemplados en esta legislación sectorial -o estén destinados a ser utilizados como componente de seguridad de estos productos-, siempre que, conforme a dicha legislación sectorial, el producto o el componente deba someterse a una evaluación de conformidad realizada por un organismo independiente. Se busca así integrar las normas del RIA en el marco de la legislación sectorial ya existente en materia de seguridad, para garantizar la coherencia y evitar duplicidades y cargas excesivas. De esta forma, los requisitos exigidos RIA se comprobarán en general como parte de los procedimientos de evaluación de conformidad previstos en las disposiciones del “nuevo marco legislativo”, con

⁴⁰ El “nuevo marco legislativo” (*New Legislative Framework* o *NLF*) al que se refiere la Propuesta de Reglamento IA se estableció mediante dos disposiciones dictadas el 9 de julio de 2008. Por una parte, la Decisión 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo, (DO L 218 de 13.8.2008, p. 82), que ofrece un modelo para la elaboración de normas sectoriales sobre seguridad y comercialización de productos en la UE. Y, por otra parte, el Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) 339/93 (DO L 218 de 13.8.2008, p. 30). Este Reglamento 765/2008 fijó los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos, si bien la parte referida a la vigilancia del mercado se suprimió para quedar regulada en el más reciente Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) 765/2008 y (UE) 305/2011 (DOUE L 169 de 25.6.2019, p. 1). La Comisión se ha planteado la conveniencia de reformar este “nuevo marco legislativo”, para lo que puso en marcha un proceso de evaluación para valorar su efectividad, eficiencia y relevancia, y en particular, entre otros aspectos, si sigue siendo útil para tratar sobre la seguridad de los productos que pueden experimentar cambios a lo largo de su ciclo de vida, como los productos inteligentes conectados, o también para valorar si fijar físicamente el mercado CE y otra información en el propio producto sigue siendo adecuado (véase el documento *Commission Staff Working Document Evaluation of the New Legislative Framework*, Brussels, 16.11.2022 SWD(2022) 364 final/2).

⁴¹ Vid. Anexo I, RIA.

la posibilidad de fijar algunos requisitos específicos sobre la integración del sistema de IA en el producto. Así, el RIA viene a complementar esa normativa sectorial para afrontar los riesgos de la IA.

Además el RIA contempla un catálogo casos de sistemas de IA independientes -en el sentido de no vinculados a esta normativa sectorial de seguridad de productos- a los que asigna también la calificación de sistemas de alto riesgo, y a los que hacemos referencia a continuación.

5. SISTEMAS DE IA DE ALTO RIESGO INDEPENDIENTES

Siguiendo las orientaciones del Libro Blanco,⁴² y de la recomendación del Parlamento Europeo,⁴³ a las que hemos hecho referencia más arriba, el Reglamento identifica una serie de sectores o ámbitos en los que se considera probable que el uso de la IA ocasione riesgos elevados y, dentro de cada uno de estos ámbitos, ciertos supuestos de uso específicos. De este modo, califica como sistemas de alto riesgo -además de los ya señalados por su vinculación a la normativa armonizada- aquellos sistemas que quedan recogidos en el listado de supuestos de sistemas de IA de alto riesgo que se contiene en el Anexo III del propio Reglamento.⁴⁴

Para elaborar este listado inicial en la propuesta de Reglamento -listado que la Comisión podrá modificar ulteriormente dentro de ciertos límites-, la Comisión siguió una metodología que tiene en cuenta si el sistema de IA en cuestión y su uso previsto genera un riesgo elevado para la salud o seguridad, o para los derechos y libertades fundamentales de las personas, aplicando una serie de criterios que se relacionan en los trabajos preparatorios.⁴⁵ Para este análisis tuvo en cuenta, entre otros, los casos de riesgo ya apuntados en el informe del Parlamento Europeo,⁴⁶ así como tipos de usos identificados en múl-

⁴² Vid. *Libro Blanco sobre la inteligencia artificial*, cit., apartado 5.C, pp. 21-22.

⁴³ *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))*.

⁴⁴ Art. 6.2 RIA.

⁴⁵ Véase el apartado 5.3 del documento de evaluación de impacto de la propuesta, en particular la nota 232 (p. 50) (en la primera parte del documento) y el Anexo 5.4 (en la segunda parte del documento): *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final (Partes 1 y 2).

⁴⁶ *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))*.

tiples estudios.⁴⁷ Los criterios para la evaluación llevada a cabo -criterios que la Comisión considera objetivos y no discriminatorios, en la medida en que tratan de modo similar los sistemas de IA similares, sin distinguir en función de su origen dentro o fuera de la UE- contemplan, entre otros aspectos, en qué medida el sistema de IA se ha utilizado o se va a utilizar; si ha causado daños a la salud, seguridad o derechos y libertades fundamentales de las personas o ha generado preocupación seria de su posible materialización; el alcance del impacto negativo de los daños y la posibilidad de afectar negativamente a una pluralidad o grupos enteros de personas; la medida en que las personas potencialmente afectadas dependen del resultado producido por el sistema -por ejemplo, si pueden o no rechazar que se les aplique-, o se hallan en una posición vulnerable frente al usuario del sistema de IA; en qué medida el resultado del sistema IA puede revertirse; si existen remedios legales efectivos; y hasta qué punto la vigente legislación de la UE es capaz de impedir o minimizar los riesgos potenciales del sistema de IA.⁴⁸

Como resultado de este análisis, la Comisión identificó en su propuesta inicial una serie de sectores y casos de uso específicos. El listado de sectores o ámbitos se ha mantenido de modo esencialmente invariado en el texto final del RIA. Concretamente, los sectores incluidos en el Anexo III del RIA son los siguientes: (1) Biometría (en la medida en que su uso esté permitido); (2) Infraestructuras críticas; (3) Educación y formación profesional; (4) Empleo, gestión de los trabajadores y acceso al autoempleo; (5) Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones; (6) Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; (7) Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; y, por último, (8) Administración de justicia y procesos democráticos. Dentro de cada uno de estos ocho ámbitos se señalan determinados usos de sistemas de IA que reciben la calificación de riesgo alto.

⁴⁷ Entre otros muchos materiales, se incluyen el informe de ISO sobre casos de uso de IA: *AI Use Cases* (ISO/IEC TR 24030), <https://www.iso.org/standard/77610.html>; datos derivados de la preparación del informe *Directrices éticas para una IA fiable*, publicado por el High-Level Expert Group On Artificial Intelligence (HLEG), 2019, <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>; resultados de la consulta pública llevada a cabo con ocasión del *Libro Blanco: la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final; etc.

⁴⁸ Vid. *supra*, nota 45.

5.1. EJEMPLOS DE CASOS DE USO RELEVANTES

El Anexo III especifica casos de usos dentro de cada uno de los ámbitos referidos, de los que destacaremos sólo algunos ejemplos, con especial mención de las novedades que el texto final incluyó respecto de la propuesta inicial.

Así, en el caso de la biometría se califican como de riesgo alto, los *sistemas de identificación biométrica remota*. Naturalmente, deben entenderse excluidos aquellos sistemas que se hallan prohibidos por aplicación del artículo 5.1.h), referidos a la identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley, a los que ya hemos hecho referencia. La texto final del RIA matiza que incluye sólo los supuestos de identificación y no los de mera “verificación” o autenticación; esto es, los casos en que no se trata de “identificar” a una persona (averiguar quién es, a partir de contrastar sus datos biométricos con los almacenados en una base de datos de referencia),⁴⁹ sino que se busca simplemente de confirmar que esa persona es quien dice ser, comparando sus datos biométricos con los ya registrados como correspondientes a dicha persona.⁵⁰ Por su parte, la mera verificación -que puede tener como finalidad, por ejemplo, permitir el acceso a un servicio, desbloquear un dispositivo o facilitar la entrada a un recinto- queda fuera del supuesto de riesgo alto incluido en el listado.⁵¹ Se incluyen también en la calificación de alto riesgo los sistemas de IA para la categorización biométrica en función de atributos o características *sensibles o protegidos*, basada en la *inferencia* de dichos atributos o características, así como los sistemas de *reconocimiento de emociones*. A este último respecto, cabe recordar que el reconocimiento de emociones en el ámbito laboral y en el ámbito educativo, por su especial potencial discriminatorio, se configuran como *prácticas prohibidas* en el artículo 5.

⁴⁹ El art. 3.35 RIA define la *identificación* biométrica como « el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos ».

⁵⁰ El art. 3.36 RIA define la *verificación* biométrica como « la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente ».

⁵¹ Cabe apuntar que, desde el punto de vista de Protección de Datos, el Comité Europeo de Protección de Datos (CEPD) considera que tanto la identificación como la autenticación o verificación suponen un tratamiento de categorías especiales de datos. Véanse las *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, versión 2.0, de 26 de abril de 2023, disponibles en https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf. La Agencia Española de Protección de Datos, que inicialmente había mantenido un criterio distinto, se ha adaptado a la posición del CEPD en su *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, de noviembre de 2023, disponible en <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>.

En relación con las infraestructuras críticas, cabe destacar que la versión final del RIA añade los sistemas de IA destinados a ser empleados como componentes de seguridad en la gestión y funcionamiento de las infraestructuras digitales críticas, además de los supuestos ya contemplados en la propuesta inicial sobre el tráfico rodado o del suministro de agua, gas, calefacción o electricidad.

En el campo de la educación y la formación profesional, la versión final del RIA añade matices, si bien lo esencial sigue siendo el uso de sistemas de IA para determinar el acceso a centros de formación y para evaluar a los alumnos y determinar los niveles formativos a los que podrán acceder. Quizás de modo más significativo se añaden como caso de riesgo alto los sistemas destinados a ser utilizados para detectar fraude en los exámenes, fraudes que ciertamente se han visto impulsados con la irrupción de las herramientas de IA generativa.

En el ámbito laboral, el texto final mantiene en lo esencial la determinación como casos de riesgo alto de los sistemas empleados para la contratación o selección de personal, con particular énfasis en la publicación de anuncios de empleo específicos y el filtrado y evaluación de solicitudes y candidatos, así como los sistemas utilizados en la evaluación del rendimiento, y toma de decisiones sobre condiciones laborales y asignación de tareas. En este último punto, la versión final destaca que se trate de asignación de tareas a partir de comportamientos individuales o rasgos o características personales.

En cuanto a los sistemas empleados para el acceso a servicios públicos y privados esenciales y para permitir el disfrute de los mismos, la versión final del RIA pone mayor énfasis en que también los servicios públicos deben ser de carácter esencial, y entre ellos incluye los de asistencia sanitaria. Cuando se trata de sistemas para evaluar la solvencia de personas físicas o establecer su calificación crediticia,⁵² la versión final elimina la excepción referida a los sistemas de IA puestos en servicio por parte de proveedores a pequeña escala para su uso propio, mientras que exceptúa de la calificación de alto riesgo el caso de los sistemas para detectar fraudes financieros. Por otra parte, añade el caso de los sistemas para evaluar riesgos y fijar precios de seguros de vida y salud.

Por lo demás se introducen variaciones en los casos de uso referidos a sistemas de IA para fines de aplicación de la ley, para migración, asilo y gestión de fronteras -excluyendo la verificación de documentos de viaje-, o para propósitos de administración de justicia y procesos democráticos. En este último ámbito se añaden como casos de alto riesgo los sistemas «para influir en el resultado de una elección o referéndum o en el comportamiento electoral de

⁵² Este tipo de sistemas puede presentar un cierto solapamiento con las prácticas que son objeto de prohibición en el art. 5.1.c) sobre *social scoring* al que nos hemos referido más arriba.

personas físicas que ejerzan su derecho de voto en elecciones o referendos», algo que naturalmente debe considerarse a la luz de las prácticas prohibidas sobre manipulación y que debe entenderse sin perjuicio del recientemente aprobado Reglamento (UE) 2024/900, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política.

5.2. CRITERIOS PARA RECHAZAR LA CALIFICACIÓN DE RIESGO ALTO

A diferencia de lo previsto en la propuesta inicial, el texto final del RIA admite que pueda considerarse que un determinado sistema de IA, a pesar aparecer incluido en el listado de casos del Anexo III, no es de alto riesgo, y que en consecuencia no rijan los requisitos y obligaciones que prevé el Reglamento para los sistemas de alto riesgo. Así, se prevé expresamente que «un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones» (art. 6.3 RIA).⁵³

Con ello se trata de evitar una catalogación automática como sistema de alto riesgo, que podría resultar desproporcionada en el caso concreto. En efecto, el catálogo del Anexo III no es más que una aproximación, que difícilmente puede asegurar que en todas las situaciones contempladas se producirá una situación efectiva de riesgo alto. En especial, el Reglamento considera que un sistema *no plantea tal riesgo* cuando no influye sustancialmente en el resultado de la toma de decisiones, es decir, que «no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada»⁵⁴. Y considera que este será el caso si se cumple *alguna* de las cuatro condiciones que recoge el artículo 6.3 RIA, y que son las siguientes.

⁵³ En una versión anterior, en lugar del adverbio “también” se empleaba la expresión “en particular”, que resultaba más ajustada a la versión inglesa, que utiliza la expresión “including”: «an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, *including* by not materially influencing the outcome of decision making». El sentido aparente es que la falta de influencia decisiva en el resultado de la decisión sería uno, entre otros, de los posibles factores que implicaría ausencia de riesgo alto del sistema. El considerando 53 señala que «pueden existir casos específicos en los que los sistemas de IA referidos en ámbitos predefinidos especificados en el presente Reglamento no entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, dado que no influyen sustancialmente en la toma de decisiones *o no perjudican dichos intereses sustancialmente*. A efectos del presente Reglamento, por sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones debe entenderse un sistema de IA que no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada» (énfasis añadido).

⁵⁴ Cfr. cdo. 53 RIA.

Primera: que el sistema de IA tenga por objeto llevar a cabo *una tarea de procedimiento limitada*. A este respecto, los considerandos ofrecen algunos ejemplos: un sistema que transforme datos no estructurados en datos estructurados; un sistema que clasifique en categorías los documentos recibidos; o un sistema que se utilice para detectar duplicados entre un gran número de aplicaciones.⁵⁵ El carácter concreto y restringido de la tarea hace que los riesgos que presenta el sistema sean limitados y que estos no aumenten por el hecho de que el sistema se emplee en uno de los ocho ámbitos considerados en el Anexo III.

Segunda: que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada. Se entiende que la mejora de esa actividad humana previa sólo puede comportar un riesgo menor.⁵⁶ Como ejemplos de este caso, los considerandos señalan los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos ya redactados -se entiende que por parte de humanos- a efectos de ajustarlo a un registro determinado, por ejemplo de carácter profesional o de naturaleza más académica, o bien para adaptarlo a una política de comunicación de marca.

Tercera: que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella. El hecho de que previamente haya tenido lugar una evaluación humana supone, a los ojos del RIA, que el riesgo del sistema no será elevado. Y apunta, como ejemplos, el uso para comprobar *a posteriori* si un profesor puede haberse desviado de su criterio general en la calificación de exámenes, o el uso para identificar otras anomalías o incoherencias en relación con decisiones previas.

Cuarta: que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el Anexo III. En este último caso lo que se considera es el riesgo que el uso de este sistema pueda representar para el resultado de la evaluación de un sistema de IA. Al limitarse a una tarea preparatoria, el Reglamento considera que su repercusión en la evaluación subsiguiente sería muy escasa desde el punto de vista del riesgo. Los ejemplos que proporcionan aquí los considerandos incluyen soluciones inteligentes para la gestión de archivos, así como sistemas de traducción de documentos.

Con independencia de estas cuatro condiciones, se dispone que en ningún caso se podrá excepcionar de su calificación como de alto riesgo aquellos

⁵⁵ Cfr. cdo. 53 RIA.

⁵⁶ Cfr. cdo. 53 RIA.

sistemas incluidos en el Anexo III que lleven a cabo la *elaboración de perfiles* de personas físicas, esto es, «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».⁵⁷

A través de la adopción de actos delegados, la Comisión podrá modificar las condiciones citadas, así como añadir nuevas, «cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del Anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas».⁵⁸ Inversamente, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales en la Unión, la Comisión adoptará actos delegados para suprimir una o más de estas condiciones que permiten considerar que el sistema no es de riesgo alto.

De la redacción del precepto resulta que el hecho de que se verifique alguna de estas cuatro condiciones -o de las que en el futuro añada la Comisión- determina por sí mismo que el sistema de que se trate, incluido en el Anexo III, *no* es de alto riesgo. El establecimiento de este nuevo automatismo no deja de ser llamativo, toda vez que la verificación de si alguna de estas condiciones se cumple puede resultar dudoso en muchos casos. Esta valoración corresponde al proveedor del sistema de IA, a quien se le exigen determinados deberes de documentación y transparencia. Así, cuando el proveedor estime -basándose en alguna de las anteriores condiciones- que su sistema *no* es de alto riesgo, deberá documentar su evaluación antes de que el sistema sea introducido en el mercado o puesto en servicio; deberá registrarlo en la base de datos de la UE en la que se registran los sistemas de alto riesgo del Anexo III;⁵⁹ y deberá facilitar la documentación de la evaluación a solicitud de las autoridades nacionales competentes.⁶⁰

Como en tantas otras materias complejas, el legislador acude al auxilio de la Comisión encomendándole que emita unas directrices que resuelvan las dificultades. Así, el RIA encarga a la Comisión que, previa consulta con el Comité Europeo de IA, elabore directrices que especifiquen la aplicación

⁵⁷ Véase el Reglamento (UE) 2016/679 (RGPD), art. 4.4; la Directiva (UE) 2016/680, art. 3.4; y el Reglamento (UE) 2018/1725, art. 3.5.

⁵⁸ Art. 6.6. RIA.

⁵⁹ Arts. 6.4, 49.2 y 71 RIA.

⁶⁰ Art. 6.4 RIA.

práctica del artículo 6, junto con -nada menos que- una lista *exhaustiva* de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.⁶¹ El alcance de este mandato resulta por lo demás algo confuso pues, mientras que el artículo 6.5 RIA, al establecerlo, se refiere en general a especificaciones sobre “la aplicación práctica del presente artículo” -por tanto, de todo el artículo 6-, el considerando 53 se refiere a estas directrices como relativas exclusivamente a la aplicación práctica de las cuatro condiciones arriba apuntadas, por las que determinados sistemas, a pesar de estar incluidos en el Anexo III no se tendrán por sistemas de riesgo alto; es decir, sólo al apartado 4 del referido artículo 6.

5.3. MODIFICACIONES DE LA RELACIÓN DE CASOS DEL ANEXO III

El listado de casos de uso de sistemas de IA podrá ser modificado por la Comisión en virtud de la autorización para adoptar actos delegados que el RIA le concede en el artículo 7. Aunque esta habilitación es una buena muestra de la flexibilidad de una normativa que se desea resistente al paso del tiempo y de la evolución tecnológica, llama la atención que se establezca como requisito para añadir nuevos casos que estos se hallen incluidos en alguno de los ocho ámbitos de actividad ya reseñados (cfr. Art. 7.1.a). Esta limitación trasluce el propósito de garantizar que la normativa no exceda de lo estrictamente necesario, sin embargo puede ir en contra precisamente de la deseada adaptabilidad -por lo menos, sin una nueva intervención del legislador de la Unión-. La modificación podrá consistir también en suprimir casos concretos de la lista cuando la Comisión considere que ya no plantean riesgos significativos y no se reduzca con ello el nivel general de protección de la salud, la seguridad y los derechos fundamentales.

Para llevar a cabo estas modificaciones, la Comisión tendrá en cuenta una compleja serie de factores, entre los que se incluyen los posibles efectos beneficiosos del sistema de IA de que se trate.

6. OBLIGACIONES DE TRANSPARENCIA FRENTE A RIESGOS DE CONFUSIÓN

Ciertos sistemas de IA quedan sujetos a obligaciones de transparencia, con independencia de si los sistemas en cuestión resultan o no de alto riesgo.

⁶¹ Art. 6.5 RIA.

No se trata pues, de un conjunto de obligaciones previsto para sistemas que ofrezcan un riesgo *inferior* a los de alto riesgo, como en ocasiones se ha presentado. Simplemente se trata de sistemas que, siendo o no de alto riesgo, pueden dar lugar a confusiones -especialmente en cuanto a la naturaleza de los resultados- que deben ser adecuadamente evitadas mediante una explicación transparente, para que resulte claro que son producto de la operación de un sistema de IA y no una creación o una actividad humana.

Estas obligaciones, dispuestas en el artículo 50, transparencia se establecen en relación con: (a) los sistemas de IA destinados a interactuar directamente con personas físicas; (b) aquellos que generen contenido sintético de audio, imagen, vídeo o texto; (c) los sistemas de reconocimiento de emociones y de categorización biométrica; (d) los que generen o manipulen contenidos de audio o vídeo que constituyan una ultrasuplantación o *deep fakes*; y (e) los que generen o manipulen texto que se publica para informar de asuntos de interés público.

En la interacción *directa* con personas físicas es esencial que la persona física sepa que no está interactuando con un ser humano sino con un sistema de IA. Por ello, el sistema deberá estar diseñado y desarrollado para que dichas personas estén informadas de este extremo. No obstante, se exceptúan los casos en que la interacción con un sistema de IA resulte evidente para una persona razonablemente informada, atenta y perspicaz.

Para los sistemas de IA generativa que den lugar a resultados en forma de audio, imagen, vídeo o texto, se exige al proveedor del sistema, con ciertas excepciones y teniendo en cuenta las circunstancias, que la información de salida esté marcada en un formato legible por máquina, y que sea posible detectar que ha sido generada o manipulada artificialmente.

Para los sistemas de reconocimiento de emociones o de categorización biométrica (siempre que no se hallen prohibidos), se exige a los responsables del despliegue informar a los afectados y tratar sus datos conforme al RGPD. También se imponen obligaciones de transparencia a los responsables del despliegue de sistemas de IA que generen o publiquen imágenes, audio o vídeo, que constituya un *deep fake* (ultrasuplantación). En concreto se les exige hacer público que esos contenidos o imágenes han sido generados o manipulados de manera artificial. La obligación se suaviza en los casos en que el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción, donde se establece que declaración se hará de modo que no dificulte la exhibición o disfrute de la obra. Cuando el contenido generado o manipulado sea texto que se publique con el fin de informar sobre asuntos de interés público, los responsables del despliegue deberán divulgar su naturaleza artificial, aunque esto no será preciso si el contenido ha sido

posteriormente revisado por un humano, y cuando una persona física o jurídica asuma la responsabilidad editorial de la publicación.

También en este campo se prevé la elaboración de códigos de buenas prácticas bajo los auspicios de la Oficina de IA.

7. RIESGOS SISTÉMICOS DE LOS MODELOS DE USO GENERAL

Nos referimos, por último, a la consideración del riesgo sistémico que se incluye en la regulación de los llamados modelos de uso general. Como se indicó más arriba, la propuesta inicial del RIA estaba marcada por el enfoque a casos de uso específicos para determinar el nivel de riesgo y no contempló los modelos y sistemas de IA que pueden aplicarse a usos muy diversos y por tanto implicar -o no-, un riesgo elevado según las circunstancias.

En particular, los llamados *modelos* son esenciales para el funcionamiento de sistemas de IA, incluso de sistemas de IA de capacidades generales, que se basan en ellos.⁶² La necesidad de abordar de algún modo tanto esos modelos como los sistemas de muy amplio espectro se hizo especialmente patente tras la irrupción de las herramientas de inteligencia artificial generativa como ChatGPT, aunque ya se había sugerido su incorporación al Reglamento con anterioridad.⁶³ La versión final del Reglamento acoge estas figuras, con la denominación de *modelos de IA de uso general* y de *sistemas de IA de uso general*. No se acoge, pues, la denominación de “modelo fundacional”,⁶⁴ que había sido sugerida por el Parlamento en sus enmiendas.

Un *modelo de IA de uso general* se define como «un modelo de IA, también uno entrenado con un gran volumen de datos utilizando la autosupervisión a gran escala, *que presenta un grado considerable de generalidad* y es *capaz de realizar de manera competente una gran variedad de tareas distintas*, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede inte-

⁶² Entre otros muchos ejemplos, Gemini (Google), GPT-4 (OpenAI), o Claude (Anthropic), se suelen considerar modelos de uso general, a partir de los cuales funcionan sistemas de IA.

⁶³ Véase, por ejemplo: Future of Life Institute: *General Purpose AI and the AI Act*, May 2022, disponible en <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf>. Otras propuestas posteriores pueden verse en HELBERGER, N; DIAKOPOULOS, N.: «ChatGPT and the AI Act», *Internet Policy Review*, 12(1), 2023, <https://doi.org/10.14763/2023.1.1682>.

⁶⁴ Ha popularizado esta denominación el Center for Research on Foundation Models (CRFM), del Stanford Institute for Human-Centered Artificial Intelligence (HAI), dedicado al estudio de estos modelos, sobre los que ha publicado diversos estudios (<https://crfm.stanford.edu/>).

grarse en diversos sistemas o aplicaciones posteriores». ⁶⁵ En cambio, un *sistema de IA de uso general* es «un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA». ⁶⁶

Como explican los considerandos, los modelos son componentes esenciales de los sistemas de IA, en los que están integrados y de los que forman parte, pero no constituyen por sí mismos un sistema de IA, pues para ello sería preciso añadirles otros componentes, como una interfaz de usuario. Por otra parte, los modelos de IA de uso general pueden introducirse en el mercado a través de APIs (*Application Programming Interface*), o mediante bibliotecas (*libraries*), ya sea como descarga directa o como copia tangible. ⁶⁷

Pues bien, dentro de los modelos de IA de uso general, se distinguen, como una subcategoría, aquellos que presentan *riesgos sistémicos*, esto es, «un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor». ⁶⁸ Estos riesgos, que son más elevados cuanto mayores sean las capacidades de los modelos, pueden surgir durante todo el ciclo de vida del modelo y están afectados por múltiples factores.

En particular, se considerará que un modelo de uso general presenta un riesgo sistémico a partir de cierto umbral de cantidad acumulada de cálculos utilizada para su entrenamiento, medida en operaciones de coma flotante, umbral que la Comisión podrá modificar para reflejar el estado actual de la técnica. ⁶⁹ Los modelos de IA de uso general de riesgo sistémico se hallan sujetos a obligaciones más rigurosas de control, evaluación, documentación, vigilancia y ciberseguridad.

⁶⁵ Art. 3.63 RIA (énfasis añadido). A fin de excluirlos de la correspondiente regulación, se exceptúan de la definición «los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización».

⁶⁶ Art. 3.66 RIA.

⁶⁷ Cfr. cdo. 97 RIA.

⁶⁸ Art. 3.65) RIA.

⁶⁹ Art. 51 RIA.

Inteligencia artificial generativa y daños por infracciones normativas del derecho de protección de datos personales. Un análisis a partir de la jurisprudencia reciente del TJUE sobre el artículo 82 RGPD

ANTONI RUBÍ PUIG¹

Profesor agregado de derecho civil, Universitat Pompeu Fabra

Sumario: 1. INTRODUCCIÓN. 2. FUNCIONAMIENTO DE LA IA GENERATIVA E IMPLICACIONES PARA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES. **2.1. Concepto.** **2.2. Tipología.** **2.3. Cadena de valor.** **2.3.1. General.** **2.3.2. Bases de datos.** **2.3.3. Modelo de IA generativa: entrenamiento y almacenamiento.** A) Entrenamiento de modelos de IA generativa. B) Almacenamiento y comunicación de modelos de IA generativa. **2.3.4. Desarrollo de sistemas basados en el modelo.** **2.3.5. Utilización del sistema.** A) *Prompts*. B) Generación de resultados. **2.3.6. Otras tareas.** 3. CUESTIONES Y PROBLEMAS SOBRE LA REPARACIÓN DE DAÑOS. **3.1. Introducción: el artículo 82 RGPD como fundamento de responsabilidad civil.** **3.2. Daños mínimos y de bagatela.** **3.3. Indemnizabilidad del temor.** **3.4. Brechas de seguridad.** **3.5. Relaciones con otros fundamentos de responsabilidad: el caso de los *deepfakes*.** **3.6. Pluralidad de sujetos responsables.** 4. CONCLUSIONES. BIBLIOGRAFÍA UTILIZADA. JURISPRUDENCIA DEL TJUE.

¹ Este capítulo se ha preparado en el marco del proyecto PID2021-126354OB-I00/MICIN/AEI/10.13039/501100011033/FEDER, UE, sobre “Responsabilidad contractual y extracontractual de las plataformas en línea” financiado por el Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación y el Fondo Europeo de Desarrollo Regional.

1. INTRODUCCIÓN

Los últimos dos años han sido testigos de importantes desarrollos y mejoras en el campo de la inteligencia artificial generativa (en adelante, «IA generativa»), que han contribuido a su popularidad y a su utilización crecientes. Sistemas y servicios como ChatGPT, Dall-E, Bard, Stable Diffusion, Midjourney, Sora o Copilot permiten a sus usuarios impartir instrucciones (*prompts*) o emplear otros *inputs* para obtener resultados sintéticos en forma de textos, imágenes, videos o código fuente informático. También bots conversacionales, asistentes virtuales e instrumentos de búsqueda se basan en modelos de IA generativa para ofrecer respuestas más complejas y de mayor calidad en las interacciones con sus usuarios. La IA generativa ha revolucionado asimismo la traducción, análisis y resumen de información. Todas estas herramientas de IA generativa se están utilizando ya en sectores tan diversos como la educación, la atención de clientes, la creación de contenidos o el ejercicio de profesiones jurídicas; y es esperable que su uso crezca en los próximos años.

El funcionamiento de los modelos y sistemas de IA generativa depende de varios elementos, pero sobre todo del acceso y uso de grandes cantidades de datos, así como de la variedad y calidad de estos. Para que un modelo pueda proporcionar unos determinados resultados mínimamente valiosos ha de haber sido entrenado previamente con bases de datos muy grandes². Previsiblemente, cuantos más datos se utilicen en su entrenamiento, mejor será la calidad del modelo y de los resultados esperables³. Aunque OpenAI se guarda de ofrecer información sobre este extremo, se estima que GPT-4, uno de los modelos más potentes que ha desarrollado, fue entrenado a partir de más de 13 millones de *tokens* provenientes de bases de datos públicas como RefinedWeb y CommonCrawl, que rastrean y almacenan información de más de 2.700 millones de páginas web. Estas mismas bases de datos u otras diferentes -por ejemplo, elaboradas internamente, a partir de datos sintéticos- pueden ser utilizadas, además de en tareas de entrenamiento, para mejorar o afinar un modelo, para desarrollar sistemas y servicios personalizados y para alinear estos con determinados objetivos de calidad. Dada la extraordinaria cantidad de datos utilizados en todas estas tareas de la cadena de valor de la

² Novelli, C., Casolari, F., Hacker, P., Spedicato, G., y Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *ArXiv, abs/2401.07348*. 1-36. pág.1.

³ Ahora bien, a partir de determinado umbral, el valor añadido que tiene sumar más datos crece a una tasa decreciente. En este sentido, véase Carrière-Swallow, Y., y Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective. *IMF Departmental Papers* 19 (16), 2019. 1-46. Además, algunos autores critican también que necesariamente cuantos más datos traten y más grandes sean los modelos de IA, mejores serán. En este sentido, véase Varoquaux, G., Luccioni, A.S., y Whittaker, M. (2024). Hype, Sustainability, and the Price of the Bigger-is-Better Paradigm in AI. (<https://doi.org/10.48550/arXiv.2409.14160>).

IA generativa, es altamente probable, sino seguro, que muchos de ellos serán datos de carácter personal y que, por tanto, su uso y, en general, el funcionamiento de modelos y sistemas comportarán actos de tratamiento de datos personales.

En estos momentos de emergencia de la tecnología, persisten muchas dudas acerca de las implicaciones jurídicas que despliega la IA generativa en el derecho de protección de datos. En la Unión Europea, son muchas las cuestiones abiertas acerca de la aplicación del Reglamento General de Protección de Datos («RGPD»⁴) a la IA generativa⁵. Las dudas no son exclusivas de este sector jurídico y se proyectan también en ámbitos tales como la responsabilidad civil y la protección de los derechos de propiedad intelectual⁶.

En el ámbito de la protección de datos personales, se han entablado recientemente varios procedimientos contra algunos de los proveedores de servicios de IA generativa más conocidos en los cuales se habrán de discutir cómo estos han de cumplir con las exigencias establecidas en el RGPD y otras normas⁷. También algunas agencias de protección de datos o autoridades de supervisión han elaborado ya guías y otros documentos acerca de las interacciones entre IA generativa y protección de datos personales⁸. En la literatura

⁴ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (OJ L 119, 4.5.2016, pgs. 1-88) (en adelante, RGPD).

⁵ Para una visión panorámica, véanse Marcos, H., y Pullin, M. (Octubre 2023). Large Language Models and EU Data Protection: Mapping (Some) of the Problems. *The Digital Constitutionalist*. <https://digi-con.org/large-language-models-and-eu-data-protection-mapping-some-of-the-problems>; Necati Pehlivan, C. (19 de septiembre de 2024). Inteligencia artificial y protección de datos. *Almacén de Derecho*. <https://almacenederecho.org/inteligencia-artificial-y-proteccion-de-datos>; y Nunez Duffourc, M., Gerke, S., y Kollnig, K. (2024). Privacy of Personal Data In The Generative AI Data Lifecycle. *New York University Journal of Intellectual Property And Entertainment Law*. Vol. 13, n. 2. 219-268.

⁶ Véanse, entre otros, Lee, K., Cooper, F., y Grimmelmann, J. (2024). Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain. *Journal of the Copyright Society*, 2024. 1-128 (en prensa) (disponible a <http://dx.doi.org/10.2139/ssrn.4523551>); y Kretschmer, M., Margoni, T. y Oruç, P. (2024). Copyright Law and the Lifecycle of Machine Learning Models. *IIC*. vol. 55. 110-138.

⁷ Para un resumen de diferentes procedimientos en marcha, véase Zanfir-Fortuna, G. (12 de septiembre de 2023). How Data Protection Authorities are De Facto Regulating Generative AI. *Future of Privacy Forum*. <https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/>. Véanse también, entre otros, Chiara, P.G. (2023). Italy: Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing. *European Data Protection Law Review*. Vol. 9. 68-72; y NYOB (6 de junio de 2024). noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI. <https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai>.

⁸ European Data Protection Supervisor (3 de junio de 2024). Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems. https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai-orientations_en_0.pdf. Véanse, en relación con agencias nacionales de protección de datos,

académica, también se discuten las implicaciones para el derecho a la protección de los datos personales de los modelos y sistemas de IA generativa⁹. A la espera de cómo vaya concretándose este entendimiento y, en particular, en el caso europeo, de cómo los desarrolladores y operadores de modelos y sistemas de IA generativa hayan de cumplir con los requisitos establecidos en el RGPD, es asumible que en su desarrollo y funcionamiento se habrán cometido ya o se podrán cometer varias infracciones de esta normativa y causar daños con ello.

El objeto de este trabajo es identificar y discutir una serie de cuestiones que pueden llegar a suscitarse en relación con la reparación de los daños y perjuicios derivados de infracciones de la normativa de protección de datos cometidas en el ámbito de la IA generativa. Este trabajo no pretende ofrecer un tratamiento completo de este tema y, principalmente, por diversas limitaciones que lo impiden.

En primer lugar, no es posible ofrecer una discusión completa de la reparación de daños por infracciones de la normativa protectora del derecho a los datos personales en el campo de la IA generativa, pues, como se verá, el cumplimiento de la normativa dependerá de cómo funcione efectivamente cada modelo o sistema en cuestión. Si bien diferentes modelos y sistemas de IA generativa pueden compartir unos ciertos rasgos comunes, en la práctica operarán de modo diferente y contarán con diseños muy diversos, algunos más respetuosos que otros en la protección de los datos personales. Por ello, si sus desarrolladores y operadores han sido escrupulosos en el cumplimiento del RGPD o han adoptado unas cautelas superiores, que descarten la ilicitud del tratamiento, no deberán responder por los daños que causen y serán los afectados quienes hayan de pechar con ellos.

En segundo lugar, en función de cómo agencias de protección de datos y tribunales acaben entendiendo algunos de los problemas de aplicación de la normativa de protección de datos al funcionamiento de la IA generativa (en

los documentos siguientes: AEPD (febrero de 2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. <https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf>; CNIL, “Les fiches pratiques sur l’IA”, 2024 (<https://www.cnil.fr/fr/les-fiches-pratiques-ia>); y Garante per la Protezione dei Dati Personali (septiembre de 2023). Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale. <https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0>.

Véanse también las orientaciones ofrecidas por la confederación de asociaciones de delegados de protección de datos: Confederation of European Data Protection Organisations (16 de octubre de 2023). Generative AI: The Data Protection Implications. *CEDPO AI Working Group*. <https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf>.

⁹ Véanse, entre otros, Ruschmeier, H. (2024). Generative AI and Data Protection. Calo, R., Ebers, M., Poncibò, C., y Zou, M. (2024). *Handbook on Generative AI and the Law*, Cambridge University Press (en prensa) (disponible en SSRN: <https://ssrn.com/abstract=4814999>).

particular, de la base de licitud para las tareas de entrenamiento de modelo), es probable que muchos de los daños esperables no sean tales o no sean indemnizables. Si, finalmente, se llega a la conclusión de que los tratamientos de datos personales y, en particular, de datos de categorías especiales, implicados en las tareas de entrenamiento de bases de datos cuentan con una base de licitud suficiente, desaparecería uno de los requisitos exigidos por el artículo 82 RGPD para fundar una pretensión indemnizatoria: no habría ya infracción normativa y, por ello, el daño si hubiera sido efectivamente sufrido por un individuo debería ser asumido por este. El legislador europeo no ha querido reducir la incertidumbre en este ámbito, como sí ha hecho en el caso de los derechos de autor mediante algunas normas del Reglamento de Inteligencia Artificial (en adelante, «RIA»)¹⁰; y, por lo tanto, hay una deferencia hacia la elaboración descentralizada del derecho de protección de datos en este ámbito y la identificación progresiva de soluciones a los diferentes problemas planteados.

En tercer lugar, la IA generativa constituye un sector dinámico, con altos niveles de innovación. Muchas de estas innovaciones se dirigen a reducir los riesgos de la IA generativa y, en particular, a los riesgos en la intimidad y el derecho a la protección de los datos personales. Por ello, es probable que se reduzcan las situaciones en las cuales se terminen causando daños y perjuicios derivados de infracciones de la normativa sobre protección de datos personales. En este sentido, en los últimos años muchos investigadores implicados en lo que se conoce como *machine unlearning* proponen y elaboran mecanismos para reducir los impactos que la IA generativa puede tener en los derechos de protección de datos¹¹.

Por último, el trabajo no persigue un examen exhaustivo de la aplicación del artículo 82 RGPD a los daños y perjuicios ocasionados por tratamientos infractores de la normativa sobre protección de datos personales en la cadena de valor de la IA generativa, sino solamente destacar algunos aspectos que puedan

¹⁰ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DO L, 2024/1689, 12.7.2024 (en adelante, «RIA»).

¹¹ Véanse, entre otros, Brown, H., Lee, K., Mireshghallah, F., Shokri, R., y Tramèr, F. (2022). What Does It Mean for a Language Model to Preserve Privacy?. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 2280-92. <https://doi.org/10.1145/3531146.3534642>; Hine, E., Novelli, C., Taddeo, M., y Floridi, L. (2023). Supporting Trustworthy AI Through Machine Unlearning. *SSRN Scholarly Paper*. <https://doi.org/10.2139/ssrn.4643518>; y Achille, A., Kearns, M., Klingenberg, C., y Soatto, S.O. (2023). AI model disgorgement: Methods and choices. *Proceedings of the National Academy of Sciences of the United States of America*, 121 (<https://doi.org/10.48550/arXiv.2304.03545>).

llegar a cobrar protagonismo en la litigación que surja en los próximos años. El trabajo no tiene, pues, una pretensión analítica y, en buena medida, se limita a identificar y describir brevemente las cuestiones jurídicas y problemas principales que permearán potenciales reclamaciones de daños y perjuicios al derecho de protección de datos personales en el campo de la IA generativa.

El trabajo se estructura del modo siguiente. Después de describir cómo funciona la IA generativa, identificar diferentes tratamientos de datos personales y su régimen jurídico básico bajo el RGPD, se presenta un conjunto de cuestiones que planteará la reparación de los daños en este ámbito de conformidad con el artículo 82 RGPD y la jurisprudencia del TJUE que lo ha interpretado. Estas cuestiones se refieren a los aspectos siguientes: la probabilidad de que los daños indemnizables lo sean por importes bajos o de bagatela; la indemnizabilidad del daño derivado del temor que datos personales puedan llegar a utilizarse maliciosamente; la causación de daños en supuestos de brechas de seguridad en el ámbito de la IA generativa; la compatibilidad de la pretensión prevista en el artículo 82 RGPD con otros fundamentos indemnizatorios; y los supuestos de pluralidad de sujetos responsables en los casos de múltiples participantes en la cadena de valor de la IA generativa. Finalmente, el trabajo presente unas breves conclusiones.

2. FUNCIONAMIENTO DE LA IA GENERATIVA E IMPLICACIONES PARA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

2.1. CONCEPTO

La IA generativa es una modalidad de inteligencia artificial que permite la producción de diferentes resultados en forma de textos, imágenes, sonidos, vídeos, código fuente informático, modelos 3D u otros datos, a partir, en general, de la entrada de un texto u otro *input*. Así, por ejemplo, algunos sistemas, como los derivados de GPT-4, pueden ser multimodales y aceptar informaciones de entrada diferentes, como, por ejemplo, textos e imágenes.

El Reglamento de Inteligencia Artificial no se refiere expresamente a la IA generativa, pero sí incluye una serie de normas aplicables a los modelos de IA de uso general (*General Purpose Artificial Intelligence Model* (GPAIM)), que fueron adoptadas durante el proceso legislativo como reacción a la popularización de ChatGPT y otros sistemas. Según el artículo 3.63 RIA un «modelo de IA de uso general» es «*un modelo de IA, también uno entrenado con un gran*

volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado».

En efecto, muchos modelos de IA generativa –y en particular, los más avanzados– que se basan en aprendizaje automatizado o *machine learning* constituirán GPAIMs. La razón principal es que estos representan modelos de lenguaje extenso (MLE) (*Large Language Models* (LLM))¹², consistentes en redes neuronales artificiales que a partir de la detección de relaciones estadísticas entre los contenidos utilizados para entrenarlos pueden llevar a cabo, entre otras, tareas de generación de textos, procesamiento y clasificación de textos y otros contenidos. Por ello, algunas normas del RIA destinadas a los GPAIMs se aplicarán a los modelos y sistemas de IA generativa. La noción de uso general o finalidad general entra en conflicto con uno de los principios rectores del RGPD: el principio de limitación de la finalidad (arts. 5.1.b) y 6.4 RGPD). No es esta la única tensión, como se verá, entre las características de la IA generativa y el armazón y espíritu que permean el sistema europeo de protección de datos de carácter personal.

2.2. TIPOLOGÍA

Encontramos dos grandes tipos de sistemas de IA, basados en modelos de uso general: por un lado, los denominados clasificatorios, discriminatorios o predictivos y, por otro lado, los generativos. Los primeros sirven para tareas de clasificación mediante la atribución de un valor a partir de una información de entrada. Por ejemplo, plataformas de contenidos como YouTube utilizan modelos discriminatorios para identificar si un determinado vídeo que quiere subir un usuario es ilícito o no. O los sistemas de asignación de un *scoring* crediticio que utilizan los bancos son también clasificatorios¹³. En los sistemas clasificatorios, los valores atribuidos por el sistema son limitados: si no son binarios, habrá un número limitado de valores que podrán asignarse. En cambio, en los sistemas de IA generativos, la respuesta no está determinada por un

¹² También, en ocasiones, estos modelos de uso general se conocen como modelos fundacionales. La terminología fue desarrollada por un grupo de investigadores de la Universidad de Stanford. Véase Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., y Liang, P. (2023). Foundation Models and Fair Use. *Stanford Law and Economics Olin Working Paper* No. 584. <https://ssrn.com/abstract=4404340>.

¹³ Véase STJUE de 7 de diciembre de 2023, asunto C-634/21, *OQ c. Land Hessen y SCHUFA Holding AG*. ECLI:EU:C:2023:957. Para un análisis del caso, véase Arroyo i Amayuelas, E. (2024). El *scoring* de Schufa. *InDret* 3.2024. 134-160.

número limitado de valores y, por tanto, no se puede predecir correctamente el resultado que ofrecerá el sistema. Esto es, a partir de un mismo *prompt*, entrada o instrucción, se pueden producir generaciones distintas, como textos o imágenes diversas que sólo se parecerían conceptualmente. La mejora de los sistemas generativos se debe sobre todo a los avances recientes en dos técnicas o arquitecturas que permiten optimizar los resultados esperables de los modelos subyacentes a partir de una descripción textual: los transformadores y la difusión¹⁴.

2.3. CADENA DE VALOR

2.3.1. General

El objeto de este apartado es presentar brevemente algunos aspectos relacionados con el funcionamiento de la IA generativa y destacar, sin ánimo de exhaustividad, algunas implicaciones para el derecho de la protección de datos¹⁵. Por ello, presentamos brevemente los diferentes elementos en el ciclo de vida o cadena de valor de la IA generativa, para mostrar que en su desarrollo y funcionamiento se llevan a cabo diferentes tratamientos de datos personales. Ello se debe en buena medida a que el RGPD parte de un concepto muy amplio de tratamiento de datos personales¹⁶. Con arreglo al artículo 4.2 RGPD, “tratamiento de datos personales” es «*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso,*

¹⁴ Por ejemplo, el modelo de ChatGPT usa técnicas de transformadores y de aquí su nombre (*Chat Generative Pre-trained Transformer*). Los modelos para generar imágenes sintéticas emplean técnicas de difusión. Véase Guadamuz, A. (2024). A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs. *GRUR International*, 73(2), 111-127. En especial, pág. 114.

¹⁵ Para un análisis más detallado de la cadena de valor desde la perspectiva de los derechos de propiedad intelectual, véanse Lee, K., Cooper, F., y Grimmelmann, J. (2024). *Op. cit.*; y Guadamuz, A. (2024). *Op. cit.*. En el ámbito de la protección de datos personales, véase Mühlhoff, R., y Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology*, 16(1), 261-292. <https://doi.org/10.1080/17579961.2024.2313794>.

¹⁶ Para Davara Rodríguez, M.A. (2021). Tratamiento (Comentario al Artículo 4.2 RGPD). Troncoso Reigada A. (Dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. Tomo I, Thomson Reuters-Civitas. 591-628, pág. 592, «*tratamiento de un dato de carácter personal es hacer cualquier cosa con el mismo*». Véase, también, STJUE de 24 febrero 2022, asunto C-175/20, *SS SIA c. Valsts ierēsmumu dienests*. ECLI:EU:C:2022:124, Apdo. 35.

cotejo o interconexión, limitación, supresión o destrucción». Se trata de un concepto claramente extenso, que comporta que la normativa prevista en el RGPD se aplique a casi cualquier tipo de uso de datos personales.

En consecuencia, las actividades relacionadas con la creación de bases de datos para el entrenamiento de modelos de IA generativa, el propio entrenamiento, el uso de un sistema de IA generativa y la producción de resultados comportarán las más de las veces tratamientos de datos personales, que habrán de cumplir con los requisitos legales establecidos en el RGPD y, en particular, con los principios generales recogidos en el artículo 5 RGPD.

Las características principales que pueden predicarse de los sistemas de IA generativa (tamaño, generalidad y opacidad) entran en clara contradicción con las líneas estructurales principales del sistema de protección del derecho de protección de datos personales establecido en el RGPD (minimización, limitación de los fines, transparencia). En consecuencia, es esperable que, salvo una intervención legislativa, en estos momentos acomodar la IA generativa al RGPD resulte ilusorio y el riesgo de infracción normativa no pueda eliminarse incluso para aquellos desarrolladores más cautelosos y que hagan esfuerzos mayores para alinear sus actividades con las obligaciones establecidas en el Reglamento.

2.3.2. Bases de datos

La cadena de valor de la IA generativa se inicia con la creación de bases de datos que luego se utilizarán para entrenar los modelos y, en su caso, para ajustarlos, corregirlos y verificar su funcionamiento óptimo. Las bases de datos utilizadas pueden ser de muchos tipos, pero, en general, suelen contener ingentes cantidades procedentes de diferentes tipos de fuentes y en formatos diferentes. Como se ha señalado, bases de datos como RefinedWeb y CommonCrawl almacenan información procedente de millones de páginas web, obtenida mediante técnicas de *scraping*. Otras bases de datos como LAION consisten en colecciones de cientos de miles de imágenes junto con una descripción textual. También proveedores de servicios de redes sociales, como Facebook, Instagram, LinkedIn o Twitter/X persiguen utilizar los contenidos generados por sus usuarios como bases de datos para desarrollar modelos de lenguaje extenso y otras herramientas de IA generativa. Es innegable que estas bases de datos contendrán datos de naturaleza personal y, por lo tanto, que su creación constituirá un tratamiento de datos cubierto por el RGPD¹⁷.

¹⁷ No se discuten en este trabajo los problemas de aplicación geográfica del Reglamento y, en particular, hasta qué punto los elaboradores de bases de datos y los entrenadores de modelos de IA

Uno de los primeros problemas que se plantea es la identificación de una base de licitud de este tratamiento de conformidad con el artículo 6 RGPD y, en caso, de tratarse datos de categorías especiales, de conformidad con el artículo 9 RGPD¹⁸.

Es cuestionable que bases de licitud como el propio consentimiento de los interesados (artículo 6.1.a) RGPD) o la necesidad para la ejecución de un contrato en el cual los interesados son parte (artículo 6.1.b) RGPD) sean adecuadas para los tratamientos requeridos para la elaboración de bases de datos. Muchas bases de datos se elaboran al margen de una relación contractual con los interesados y, además, a partir de técnicas masivas de *webscraping* que hacen inviable cualquier posibilidad de recabar la autorización o consentimiento de las personas afectadas.

Por ello, fuera de una previsión legal específica, la base de licitud que, de entrada, parece más adecuada para la elaboración de bases de datos a utilizar en la cadena de valor de la IA generativa es la satisfacción de intereses legítimos del compilador de la base de datos o en su caso de otro sujeto, como el desarrollador del modelo. El artículo 6.1.f) RGPD prevé que el tratamiento de datos personales será lícito si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales. Según la jurisprudencia del TJUE, este precepto establece tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero persigan un interés legítimo; segundo, que el tratamiento de los datos personales sea necesario para la satisfacción de ese interés legítimo, y, tercero, que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado en la protección de los datos¹⁹. En suma, será necesaria una ponderación de dere-

generativa situados fuera de la UE han de cumplir con el RGPD, si finalmente lo que se explota en la Unión es un sistema basado en aquellos. Véase artículo 3 RGPD.

¹⁸ Según el artículo 9.1 RGPD constituyen categorías especiales de datos personales, dotados de un régimen jurídico más protector, aquellos «que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física».

¹⁹ Véanse, entre otras, STJUE de 17 de junio de 2021, asunto C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, ECLI:EU:C:2021:492, apdo. 106; STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 106; y STJUE de 12 de septiembre de 2024, asuntos acumulados C-17/22 y C-18/22, *HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG c. Müller Rechtsanwalts-gesellschaft mbH y otros*, ECLI:EU:C:2024:738, apdo. 49. En la literatura española, véase Gil González, E. (2022). *El interés legítimo en tratamientos de datos personales*. La Ley.

chos e intereses, que plantea diversos interrogantes, entre ellos, cómo se han de valorar las expectativas razonables de los titulares de datos personales²⁰; o hasta qué punto hay que considerar o no los beneficios y riesgos que puede conllevar el desarrollo futuro de modelos y sistemas de IA generativa o si únicamente se han de contemplar en la ponderación los relacionados con la propia elaboración de la base de datos, particularmente cuando las diferentes tareas son llevadas a cabo por sujetos diferentes en la cadena de valor de la IA generativa. El RGPD no descarta que el interés legítimo pueda derivar de un ejercicio de la libertad de empresa reconocida en el artículo 16 CDFUE y, por ello, es irrelevante de entrada que tanto la elaboración de la base de datos como su uso posterior para entrenar modelos de IA generativa tengan una finalidad comercial. Ahora bien, hay que tener en cuenta que muchas de las bases de datos que se están utilizando para entrenar modelos de IA generativa han sido elaboradas por entidades sin ánimo de lucro con finalidades de investigación científica²¹.

Por otra parte, si la base de datos incluye categorías especiales de datos, será necesario contar con una de las bases de licitud previstas en el artículo 9 RGPD²². Este precepto no prevé específicamente una base de licitud basada en la satisfacción de los intereses legítimos del responsable del tratamiento o de un tercero. Por ello, de entrada, en la elaboración de las bases de datos,

²⁰ Véase considerando 47 RGPD.

²¹ Véanse artículos 9.2.j) y 89 RGPD.

²² Obsérvese que el RIA solamente se refiere a la posibilidad de tratar datos de categorías especiales de un modo doblemente limitado: la previsión cubre únicamente sistemas de IA de alto riesgo y para la finalidad específica de detección y corrección de sesgos. Véase artículo 10.5 RIA: «En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes: a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos; b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización; c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas; d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos; e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior; f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos».

el responsable deberá adoptar las medidas técnicas necesarias para evitar la recopilación de datos sensibles no relevantes, por ejemplo, implementado filtros que impidan la copia de determinadas categorías de datos o la no inclusión en las tareas de *scraping* de determinadas páginas web que previsiblemente contengan datos sensibles²³.

La adopción de tales medidas puede contribuir a evitar la ilicitud del tratamiento. El derecho a la protección de los datos personales no es un derecho absoluto y han de considerarse también las posibilidades del responsable para reducir el impacto negativo de sus actividades: no resulta viable y óptimo, como ha señalado el TJUE, que un buscador de internet elimine todos los datos de categorías especiales antes de mostrar sus resultados²⁴. A pesar de las diferencias, esta consideración en relación con los buscadores de internet podría llegar a predicarse de las bases de datos elaboradas y utilizadas en el ámbito de la IA generativa. En cualquier caso, ha recordado el TJUE, el responsable deberá reaccionar frente al ejercicio de derechos por parte de los interesados frente al tratamiento de sus datos sensibles.

Por otra parte, el artículo 9.2.e) RGPD legitima los tratamientos referidos a datos personales que el interesado ha hecho manifiestamente públicos. Con todo, habrá que valorar, caso por caso, si los usuarios en cuestión de un sitio web o de una aplicación que introdujeron voluntariamente datos sensibles, habían consentido explícitamente, sobre la base de una información expresa facilitada por ese sitio o esa aplicación antes de tal introducción o activación, que dichos datos podrían ser visualizados por cualquier persona que tuviera acceso al citado sitio o a la referida aplicación²⁵. Es dudoso, además, que las expectativas razonables de los usuarios puedan referirse al mismo tiempo a la aceptación de que terceros puedan elaborar bases de datos con su información y que estas puedan servir luego para entrenar modelos de IA generativa.

La enorme cantidad de datos tratados por medios automáticos las más de las veces entra en conflicto con el modelo individualista establecido en el sistema europeo de protección de datos europeos, que confía en una identificación de los diferentes datos tratados y la salvaguardia de los derechos de los individuos en relación con ellos. Hay claramente una tensión entre el número masivo de datos tratados en el ámbito de la IA generativa y el principio

²³ También puede resultar pertinente llevar a cabo una evaluación de impacto de conformidad con lo previsto en el artículo 35 RGPD, como medida adicional de mitigación de riesgos.

²⁴ STJUE de 24 de septiembre de 2019, asunto C-136/17, *GC y otros c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773, apdo. 37.

²⁵ STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 83.

de minimización. Ello se percibe también en las tareas de anotación llevadas a cabo en los procesos de elaboración de bases de datos. A la hora de añadir información valiosa a los diferentes datos recogidos y que también puede ser utilizada junto a estos para entrenar un modelo de IA generativa, será necesaria adoptar las medidas adecuadas para cumplir con los principios de minimización y de exactitud de los datos personales, previstos respectivamente en los artículos 5.1.c) y d) RGPD.

2.3.3. Modelo de IA generativa: entrenamiento y almacenamiento

A) *Entrenamiento de modelos de IA generativa*

A continuación, en la cadena de valor, encontramos el modelo propiamente dicho, que puede concebirse como un conjunto de técnicas y algoritmos, que a partir de una serie de pesos y variables puede utilizarse para obtener unos resultados. Existen tres características principales que pueden predicarse de estos modelos: escalabilidad, autonomía y opacidad.

Este modelo se entrena con una o más bases de datos, para que aprenda mecánica y autónomamente a detectar relaciones estadísticas o patrones en los datos y entre ellos. El entrenamiento de un modelo exige muchos recursos de tiempo y energía. Se entiende que el entrenamiento comporta actos de tratamiento de datos personales y, por tanto, deberá contar con una base de licitud y cumplir con los principios y los deberes que el RGPD impone a los responsables²⁶. En buena medida, todo lo señalado en el apartado anterior referido a la elaboración de las bases de datos puede trasladarse al entrenamiento de los modelos de IA generativa.

Dependiendo de las técnicas de entrenamiento utilizado, es posible que los datos personales se anonimicen a partir del uso de técnicas como *differential privacy* o *federated machine learning*. La anonimización constituye un tratamiento de datos específico que requiere también de una base de licitud²⁷. En cualquier caso, es importante considerar si efectivamente los datos son anonimizados o únicamente pseudonimizados.

²⁶ Véase, en general, Hacker, P. (2021). A legal framework for AI training data-from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, 13(2), 257-301. <https://doi.org/10.1080/17579961.2021.1977219>.

²⁷ En general, la base de licitud será la satisfacción del interés legítimo del responsable del tratamiento. Ruschemeier, H. (2024). *Op. cit.*, pág. 8.

B) Almacenamiento y comunicación de modelos de IA generativa

Una de las cuestiones inciertas en este ámbito se refiere a la calificación jurídica de los actos de almacenamiento y comunicación de modelos de IA generativa como posibles tratamientos de datos personales. Se ha defendido que, después de entrenado un modelo de lenguaje extenso, el modelo no contiene ya datos personales, pues la información se conserva en un formato de *tokens* y *embeddings*, esto es, fragmentos que, después de anonimizar los datos, carecen de significado y son solo representaciones matemáticas que persiguen reflejar correlaciones entre diferentes elementos a partir de pesos y variables²⁸. Se trataría de información agregada que no permitiría la identificación de un interesado²⁹. Ahora bien, el hecho de que los sistemas de IA generativa puedan producir *outputs* que reproducen datos que se utilizaron en el entrenamiento del modelo³⁰ lleva a algunos autores a cuestionar que los modelos no contengan y no almacenen datos personales³¹. Las diferencias entre los diferentes tipos de modelos y, en particular, si están basados en transformadores o difusión, puede ser relevante en relación con el tipo de información finalmente almacenada y si efectivamente aquellos incluyen o no datos de carácter personal.

Si el modelo de IA generativa no almacena datos de carácter personal, su proveedor no deberá, por ejemplo, atender a peticiones de interesados que quieran ejercer sus derechos conforme al RGPD, por ejemplo, en relación con la supresión o rectificación de datos o la oposición al tratamiento.

²⁸ Hamburg Commissioner for Data Protection and freedom of information (2024). Discussion Paper: Large Language Models and Personal Data. https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf. Pág. 5.

²⁹ Sobre el concepto de dato personal y el test de la identificabilidad, véanse, en la jurisprudencia del TJUE, STJUE de 19 de octubre de 2016, asunto C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*. ECLI:EU:C:2016:779; STJUE de 20 de diciembre de 2017, asunto C-434/16, *Peter Nowak c. Data Protection Commissioner*. ECLI:EU:C:2017:994; STJUE de 8 de diciembre de 2022, asunto C-180/21, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*. ECLI:EU:C:2022:967; STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*. ECLI:EU:C:2023:370; STJUE de 9 de noviembre de 2023, asunto C-319/22, *Gesamtverband Autoteile-Handel eV c. Scania CV AB*. ECLI:EU:C:2023:837; y STJUE de 7 de marzo de 2024, asunto C-604/22, *IAB Europe c. Gegevensbeschermingsautoriteit*. ECLI:EU:C:2024:214.

³⁰ Carlini, N., Tramer, F., Wallace, E., Jagielski, M. et al. (2021). Extracting Training Data from Large Language Models. *30th USENIX Security Symposium*. <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>. 2633-2650; Staab, R., Vero, M., Balunović, M. y Vechev, M. (2023). Beyond Memorization: Violating Privacy Via Inference with Large Language Models. <https://arxiv.org/abs/2310.07298>.

³¹ Ruschemeier, H. (2024). *Op cit.* Pág. 6.

El RIA impone una serie de obligaciones a los proveedores de sistemas de IA de alto riesgo relativas a la gobernanza de datos, que en algunos casos podrán llegar a afectar a modelos y sistemas de IA generativa³². Además, con arreglo al artículo 53.1.d) RIA, los proveedores de GPAIMs «elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA». Dependiendo del tipo de detalle de la información suministrada, este deber puede comportar un nuevo acto de tratamiento de datos personales.

2.3.4. Desarrollo de sistemas basados en el modelo

A continuación, el modelo se puede desarrollar, esto es, puede transformarse en un servicio utilizable por terceros. Esto puede hacerse, por ejemplo, mediante una interfaz de usuario con un robot de conversación como hace ChatGPT o mediante una aplicación informática, entre otros. De entrada, el modelo se podrá utilizar para usos y finalidades muy diversas y se pueden desarrollar sistemas que se dirijan a una finalidad concreta (por ejemplo, generación de contenidos sintéticos, servicios de traducción, servicios de clasificación de imágenes, entre otros). El modelo se puede licenciar a un tercero, para que sea éste el que desarrolle los servicios específicos. De ahí que el RIA distinga entre modelos y sistemas de IA. En este sentido, según el artículo 2.1 RIA, un sistema de IA es *«un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la forma de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales»*.

El desarrollo de estos sistemas puede implicar nuevos actos de tratamiento de datos personales, en función de cómo se lleve a cabo. En muchos supuestos, las tareas de personalización y de *fine-tuning* podrán recurrir a nuevas bases de datos, en algunos casos de titularidad del propio desarrollador del sistema, y, en consecuencia, deberán contar con una base de licitud y cumplir con la normativa establecida en el RGPD.

Un problema potencial que puede plantearse es el relativo a los modelos divulgados en abierto que pueden ser desarrollados por cualquiera, sin necesidad de que el titular del modelo lleve a cabo un control o selección o reciba contraprestación alguna por la licencia. Es cuestionable que, si el desarrollador del modelo ha infringido la normativa sobre protección de datos,

³² Véase artículo 10 RIA.

por ejemplo, al entrenar su modelo sin contar con una base de licitud, haya de responder por nuevas infracciones que puede llevar a cabo un tercero que desarrolla el modelo para integrarlo en sus productos y servicios. Ahora bien, ello no excluye, como se verá, que la responsabilidad civil derivada de sus propias infracciones normativas cubra el daño moral ocasionado a un individuo por el temor que el tercero en cuestión lleve a cabo unos usos maliciosos del modelo que puedan afectar negativamente a sus datos personales³³.

2.3.5. Utilización del sistema

A) *Prompts*

El modelo desarrollado o implementado puede utilizarse para producir las generaciones. En este sentido, los usuarios que tengan acceso al sistema y a los servicios que éste ofrezca pueden redactar instrucciones (*prompts*) para obtener textos, imágenes, sonidos u otros tipos de contenidos. Estos *prompts* pueden contener datos personales, tanto del propio usuario como de terceros. Además del propio funcionamiento inmediato del sistema, el desarrollador o el operador del modelo pueden llegar a tratar estos datos para otras finalidades (por ejemplo, para tareas de moderación de contenidos o para entrenar el modelo) y pueden llegar a almacenarlos o a utilizarlos para la mejora del modelo o sistema.

El primer supuesto es menos problemático. El usuario del sistema seguramente, al haberse dado de alta para ser destinatario de los servicios, habrá prestado su consentimiento a los diferentes tratamientos de sus datos personales. En otros términos, el tratamiento de datos del usuario destinatario de los servicios del sistema de IA generativa estará basado en el consentimiento de conformidad con los artículos 6.1 y 7 RGPD o, en su caso, el artículo 9.2.a) RGPD. El responsable del tratamiento habrá de adoptar todas las medidas para cumplir con sus obligaciones de responsabilidad activa de conformidad con el RGPD. En el caso de datos de terceros, el usuario no puede prestar el consentimiento en nombre del tercero y puede plantearse la duda de cuál ha de ser la base de licitud para la introducción y recogida de estos datos. En segundo lugar, en este último caso, se puede plantear el problema de la atribución de roles entre las diferentes personas implicadas y, en particular, si ha de considerarse al usuario del sistema de IA generativa que trata datos de terceros en forma de *inputs* como responsable del tratamiento único y al operador como encargado o corresponsable del tratamiento.

³³ Véase *infra* apdos. 3.2 y 3.3.

En particular, con arreglo a la jurisprudencia del TJUE, aunque pueda establecerse un supuesto de corresponsabilidad en el tratamiento, la calificación quedaría limitada a los actos relativos a la introducción de los datos y no a las tareas posteriores que pudiera llevar a cabo el operador³⁴.

B) Generación de resultados

Los sistemas de IA generativa pueden producir diferentes tipos de resultados (*outputs*). Por ejemplo, pueden obtenerse imágenes de personas sintéticas, esto es, retratos digitales de personas no reales, que se utilizan luego en la publicidad, catálogos u otras ilustraciones. Al no tratarse de personas físicas concretas, estas imágenes no comportarán comunicación de datos personales.

En otras ocasiones, los resultados ofrecidos por un sistema de IA generativa pueden incluir datos personales. Por ejemplo, un usuario puede solicitar información acerca de él mismo y obtener una información incorrecta o que puede afectar a su privacidad. Aunque no necesariamente este fenómeno responde a que el modelo se entrenó con datos personales del afectado, en muchos casos esto será así³⁵. En este último caso, se habla de “memorización” o *overfitting*, esto es, la posibilidad que, de algún modo, las generaciones producidas por un sistema repliquen datos que se utilizaron en el entrenamiento del modelo subyacente. En la literatura técnica se han descrito diferentes razones que pueden contribuir a este fenómeno, como limitaciones en la base de datos utilizada para entrenar el modelo, duplicados y otros tipos de copias de datos incluidas en la base empleada para entrenar el modelo, la propia complejidad del modelo, o datos de baja calidad que el modelo no puede distinguir de otros relevantes.

Sea como sea, la generación de estos resultados y su puesta a disposición suponen un acto de tratamiento de datos personales. Entre otros aspectos,

³⁴ En este sentido, véanse STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH /Facebook Ireland Ltd/Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*. ECLI:EU:C:2018:388; STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyskunta*. ECLI:EU:C:2018:551; STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629; y STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcija*. ECLI:EU:C:2023:949.

³⁵ En la literatura técnica, véanse, entre otros, Carlini, N., Hayes, J., Nasr, M., Jagielski, M., Sehwag, V., Tramèr, F., Balle, B., Ippolito, D., y Wallace, E. (2023). Extracting Training Data from Diffusion Models. *ArXiv, abs/2301.13188*; El-Mhamdi, E., Farhadkhani, S., Guerraoui, R., Gupta, N., Hoang, L.N., Pinot, R., y Stephan, J. (2022). On the Impossible Safety of Large AI Models. *ArXiv, abs/2209.15259*; y Gupta, M., Akiri, C., Aryal, K., Parker, E., y Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access, 11*, 80218-80245.

pueden destacarse los derechos que corresponden al usuario frente al operador del sistema de IA: el derecho de acceso (artículo 15 RGPD); el derecho de rectificación (artículo 16 RGPD) y el derecho de supresión (artículo 17 RGPD).

La producción de resultados por los sistemas de IA generativa también puede llegar a inferir y revelar datos de categorías especiales. El TJUE ha señalado que el tratamiento de datos personales por parte del operador de una red social en línea como Facebook, consistente en la recogida, mediante interfaces integradas, cookies o tecnologías de almacenamiento similares, de los datos resultantes de la consulta de esos sitios y aplicaciones, así como de los datos introducidos por el usuario, en la puesta en relación del conjunto de esos datos con la cuenta de la red social de este y en la utilización de dichos datos por el operador comporta un tratamiento de categorías especiales de datos personales (artículo 9.1 RGPD)³⁶. No es descartable que ello también ocurra con los servicios de generación de *outputs* mediante IA generativa.

Es habitual que los desarrolladores de modelos de IA generativa utilicen los diferentes *outputs* producidos como datos sintéticos que pueden añadirse a sus bases de datos para ser utilizados en nuevos entrenamientos u otras tareas de corrección de errores y mejora de calidad. Previsiblemente, si estos datos sintéticos incluyen datos personales, estos usos comportarán nuevos tratamientos, para los cuales el responsable deberá cumplir con las disposiciones establecidas en el RGPD.

Podemos destacar tres problemas adicionales con los resultados generados por sistemas de IA generativa. El primero de ellos se refiere a la generación de alucinaciones o resultados incorrectos. Es posible que un resultado generado incluya información falsa, incorrecta, insuficiente o desfasada sobre un individuo. Ello puede deberse, por ejemplo, a que el modelo fue entrenado con datos antiguos, que no reflejan cambios acaecidos más recientemente. En consecuencia, puede transgredirse el principio de exactitud (art. 5.1.d) RGPD). Deberán ofrecerse vías a los posibles afectados para ejercer su derecho de rectificación conforme al artículo 16 RGPD. El segundo de los problemas se refiere a la generación de resultados especialmente dañinos para derechos de la personalidad de un individuo y, en particular, de resultados sintéticos que, por sus características, puedan constituir intromisiones ilegítimas en sus derechos al honor, intimidad o propia imagen. Un ejemplo de ello serán las denominadas ultrasuplantaciones (*deepfakes*). Con arreglo al artículo

³⁶ STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 73. Véase también STJUE de 1 de agosto de 2022, asunto C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601.

3.60 RIA, estas se definen como «*un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos*». Aunque el RIA establece únicamente deberes de transparencia (art. 50.4 RIA), si las ultrasuplantaciones causan daños a una persona física, se plantea la cuestión acerca del fundamento de la pretensión indemnizatoria³⁷. El tercer problema concierne a la posterior utilización del *output* obtenido: si este se llega a emplear para la adopción de decisiones solamente automatizadas, sin supervisión humana, resultará de aplicación lo establecido en el artículo 22 RGPD.

Por último, puede destacarse que la producción de resultados mediante IA generativa relacionados con un individuo puede constituir un indicio de que el modelo fue entrenado con datos personales de aquel. Si bien este individuo debe poder ejercer sus derechos previstos en los artículos 13 a 22 RGPD, es muy probable que sus pretensiones no sean factibles. Por ejemplo, es dudoso que pueda ejercerse de forma efectiva un derecho de supresión o al olvido³⁸ o que se objete a determinados tratamientos llevados a cabo en el desarrollo de los modelos y sistemas de IA generativa. Ello se debe a que no es factible económicamente proceder a una supresión de datos personales en una base de datos para luego entrenar de nuevo el modelo con el objetivo de que no obtenga información de tales datos.

2.3.6. Otras tareas

Un modelo de IA generativa puede ser objeto de ajustes, corrección de deficiencias o evitación de algunos tipos de resultados. Esto es, los responsables del sistema pueden llevar a cabo tareas de moderación de los contenidos generados por el sistema, por ejemplo, para evitar que sean infractores de derechos o ilícitos de algún otro modo. El ajuste puede acarrear nuevos entrenamientos del modelo, por ejemplo, con nuevas bases de datos o bases modificadas o purgadas. También, en la cadena de valor, el desarrollador de un sistema de IA generativa puede decidir emprender tareas para su alineación, esto es, un refinamiento de éste para cumplir con determinados objetivos de calidad.

Todas estas tareas pueden implicar nuevos usos de datos personales y, por ende, de actos de tratamiento cubiertos por el RGPD. Con arreglo al principio de minimización y de privacidad desde el diseño, resulta recomendable evitar

³⁷ Véase *infra* apartado 3.5.

³⁸ Véase, por ejemplo, Chang, C. (2024). When AI Remembers Too Much: Reinventing The Right To Be Forgotten For The Generative Age. *Washington Journal of Law and Technology and the Arts*, 19(3) 22-45.

el uso de datos personales, especialmente, si se pueden realizar estas tareas con datos sintéticos o con datos totalmente anonimizados.

3. CUESTIONES Y PROBLEMAS SOBRE LA REPARACIÓN DE DAÑOS

3.1. INTRODUCCIÓN: EL ARTÍCULO 82 RGPD COMO FUNDAMENTO DE RESPONSABILIDAD CIVIL

El desarrollo y funcionamiento de los modelos y sistemas de IA generativa pueden comportar la comisión de diversas infracciones normativas en el ámbito de la protección de datos personales: hay un riesgo de que los tratamientos de datos personales implicados no siempre cumplirán con lo establecido en el RGPD. Ello dependerá, en buena medida, primero, de cómo las agencias y tribunales vayan construyendo progresivamente el entendimiento acerca de las implicaciones que despliega el derecho de protección de datos en la IA generativa y si son más o menos estrictos y, segundo, de las propias características de cada sistema y modelo. Cada caso deberá examinarse individualmente por cuanto habrá desarrolladores y operadores que de buen inicio habrán invertido más esfuerzos y recursos en hacer sus productos y servicios más respetuosos con la normativa protectora de los datos personales (protección de datos desde el diseño y protección por defecto (artículo 25 RGPD)) y otros menos cuidadosos que habrán adoptado decisiones más arriesgadas. En cualquier caso, es posible que en el desarrollo y funcionamiento de los modelos y sistemas de IA generativa se causen daños y perjuicios a usuarios y terceros.

El artículo 82 RGPD establece un fundamento de responsabilidad para la compensación de los daños derivados de infracciones normativas del derecho de protección de datos y, por ello, es probable que en los próximos años afectados por modelos y sistemas de IA generativa recurran a este precepto para fundar al menos algunas de sus pretensiones resarcitorias y, en particular, aquellas relativas a perjuicios que formen parte del ámbito de protección de las normas infringidas. Según el artículo 82.1 RGPD, *«[t]oda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos»*³⁹.

³⁹ Para una discusión del precepto, véase Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, 5 (4), 53-87.

En los dos últimos años, el TJUE ha dictado varias sentencias en las cuales ha ido interpretando el artículo 82 RGPD y, en la actualidad, penden también varias cuestiones prejudiciales, que, luego de resueltas, acabarán perfilando cómo ha de funcionar la reparación de los daños derivados de infracciones normativas en materia de protección de datos personales. Hasta la fecha, el Tribunal ha sido muy claro en señalar que este precepto incluye unos requisitos cumulativos que han de acreditarse para que prospere una pretensión indemnizatoria basada en él: la comisión de una infracción del Reglamento, el padecimiento de daños y perjuicios materiales o inmateriales, y una relación de causalidad entre la infracción y dichos daños y perjuicios⁴⁰. Esta comprensión jurisprudencial va a tener que aplicarse en los próximos años a las diferentes pretensiones indemnizatorias que ejerzan individuos que consideren que sus datos personales hayan sido afectados por modelos y sistemas de IA y que con ello hayan sufrido daños.

El incremento en el uso de modelos y sistemas de IA generativa y sus tratamientos de datos personales comportarán con alta probabilidad algunos retos para la gestión de los daños y su compensación. Hay, al menos, tres cualidades que podrán acompañar a los daños y perjuicios asociados con modelos y sistemas de IA generativa y modelos similares: su carácter masivo, pues es probable que una misma operación o un mismo sistema afecten a grandes grupos de población; su naturaleza cumulativa, pues si bien el impacto inicial sobre la esfera de un individuo puede ser mínimo, la escalabilidad, repetición y ampliación que permiten las tecnologías digitales resultan en un incremento de su alcance y gravedad⁴¹; y la posibilidad de que se proyecten reticularmente, esto es, que, aprovechando los efectos de red (*network effects*) que presentan muchas tecnologías de inteligencia artificial, afecten a sujetos diferentes a la víctima primaria⁴². Estas características anticipan una potencial avalancha de reclamaciones indemnizatorias para las cuales el sistema de responsabilidad civil extracontractual, y, en particular, el artículo 82 RGPD, no está seguramente bien equipado⁴³. Otros retos derivarán de la implicación de varios

⁴⁰ STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370, apdo. 32; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 34; y STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*, ECLI:EU:C:2024:536, apdo. 22.

⁴¹ Famularo, J. (2023). Platform-Related Harms., *Yale-Wikimedia Initiative on Intermediaries & Information*, 1-14. https://law.yale.edu/sites/default/files/area/center/isp/documents/platform-relatedharms_issessayseries_2023.pdf. Págs. 8-9.

⁴² Es lo que los profesores Anna Beckers y Gunther Teubner han denominado “daños por interconectividad” (*interconnectivity damages*). Véase Beckers, A., y Teubner, G. (2021). *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds*. Hart, 161-162.

⁴³ Sobre ello, Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Álvarez Lata, N. (2024). *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*. APPDC-Aranzadi. 621-688.

agentes en la cadena de valor de la IA generativa y de los riesgos relacionados con la ciberseguridad.

3.2. DAÑOS MÍNIMOS Y DE BAGATELA

El carácter masivo del impacto negativo que pueden desplegar los modelos y sistemas de IA generativa en miles, sino millones, de individuos cuyos datos personales fueron utilizados para tareas de entrenamiento sin contar con una base de licitud o infringiendo de otro modo el RGPD puede comportar que un gran número de víctimas y otros perjudicados acaben sufriendo daños de diversa índole. Acaso en la esfera individual, el daño puede ser mínimo. De hecho, es asumible que el valor patrimonial de los propios datos personales es ínfimo o nulo: los datos de un sujeto específico no presentan un valor idiosincrático para quien quiere elaborar una gran base de datos o entrenar un modelo de IA generativa; son fungibles con otros y, por ello, prescindibles. El responsable del tratamiento está interesado únicamente en disponer de cuantos más datos mejor. Por otra parte, el daño moral de conocer que los datos de uno han sido incluidos en una base de datos utilizada luego para entrenar un modelo de IA generativa también puede ser escaso o limitado. En suma, las pretensiones indemnizatorias en este sector pueden serlo por cantidades modestas.

En determinados ordenamientos y regímenes particulares, hay reglas que impiden la reparación de estos daños insignificantes, por ejemplo, mediante el establecimiento de umbrales (*de minimis*). El objetivo principal es evitar una avalancha de reclamaciones de escasa cuantía (*Bagatelklagen*) que saturen el sistema judicial de responsabilidad civil extracontractual y, por ello, suelen ponerse límites a perjuicios que suelen presentarse de forma dispersa y alcanzar a una clase más o menos indeterminada de víctimas. Así ocurre, por ejemplo, con algunos supuestos de daño moral autónomo y de daños económicos puros⁴⁴.

En aplicación del artículo 82 RGPD, el TJUE ha señalado, sin embargo, que el principio de reparación efectiva fundamenta el derecho a ser compensado por el daño realmente sufrido, con independencia de su cuantificación. Esta fue una de las primeras cuestiones resueltas por el TJUE en la primera de las sentencias dictadas en interpretación del artículo 82 RGPD, la de 4 de mayo de 2023, en el asunto *Österreichische Post*⁴⁵.

Los hechos del caso fueron los siguientes. «Österreichische Post», una compañía austríaca dedicada a la edición de listines telefónicos y venta de ba-

⁴⁴ Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Especialmente, pp. 664-672.

⁴⁵ STJUE de 4 de mayo de 2023, asunto C-300/21, *UI v. Österreichische Post AG*, ECLI:EU:C:2023:370.

ses de datos postales, utilizaba desde el 2017 un algoritmo para identificar las afinidades políticas de ciudadanos de aquel país. Su objetivo era confeccionar grupos de sujetos para luego comercializarlos a anunciantes.

Un ciudadano austríaco descubrió que la compañía había inferido con este algoritmo su afinidad política con un determinado partido de aquel país. Si bien este dato inferido no fue comunicado a terceros, ni utilizado con ninguna finalidad, el individuo consideró que la atribución de esta afinidad política le había supuesto «una importante contrariedad, una pérdida de confianza y un sentimiento de humillación». Por ello, inició un proceso judicial en el cual solicitó que se cesara en el tratamiento de sus datos y reclamó una indemnización de 1.000 euros en concepto de daño moral. Los tribunales internos denegaron la pretensión indemnizatoria al considerar que, en el derecho austríaco, se exige un determinado umbral de gravedad para que pueda prosperar y que no era suficiente con los meros sentimientos negativos experimentados por el actor. El Tribunal Supremo austríaco (*Oberster Gerichtshof*) suspendió el procedimiento y planteó diferentes cuestiones prejudiciales al TJUE. En particular, inquirió acerca de si la exigencia de un umbral mínimo de gravedad era compatible o no con el artículo 82 RGPD.

Para el TJUE, el derecho a indemnización establecido en el artículo 82 RGPD no está supeditado a que los daños y perjuicios considerados alcancen un determinado umbral de gravedad. Para el Tribunal, condicionar la indemnización a haber superado un determinado límite cuantitativo o cualitativo podría afectar a la aplicación coherente y uniforme del régimen jurídico armonizado en el RGPD, ya que jueces y tribunales de diferentes tribunales podrían adoptar soluciones diversas⁴⁶.

Si bien las reglas sobre cuantificación de los importes indemnizatorios corresponden al derecho nacional de los EE.MM. en virtud del principio de autonomía procesal, las autoridades nacionales han de respetar los principios de equivalencia y efectividad del derecho europeo. Una regla *de minimis*, que estableciera únicamente la indemnizabilidad de los importes que superaran determinado importe, podría llegar a transgredir el principio de efectividad, ya que podría llegar a hacer imposible en la práctica o excesivamente difícil el ejercicio de los derechos establecidos en el artículo 82 RGPD, que consagra una regla de reparación integral del daño y permite la compensación de una «indemnización total y efectiva por los daños y perjuicios sufridos» (Considerando 146 RGPD)⁴⁷. El TJUE ha reiterado esta doctrina en otros asuntos⁴⁸.

⁴⁶ Apdo. 49.

⁴⁷ Apdos. 56-58.

⁴⁸ STJUE de 14 de diciembre de 2023, asunto C-456/22, *VX, AT c. Gemeinde Ummendorf*, ECLI:EU:C:2023:988, apdo. 23; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*,

En consecuencia, es posible que las infracciones del derecho de protección de datos cometidas en el campo de la IA generativa lleven aparejadas la causación de daños masivos a un conjunto muy elevado de víctimas y que una porción no desdeñable de ellas entable pleitos para solicitar una indemnización pecuniaria relativamente baja o simbólica. Esta situación habrá de conllevar problemas de gestión del sistema de reparación. En otros términos, el artículo 82 RGPD no impide que cualquier afectado que pueda acreditar un daño mínimo relacionado con la infracción de normas del RGPD y ocurrido en el desarrollo y funcionamiento de un modelo o un sistema de IA generativa pueda formular una demandada de responsabilidad civil antes los juzgados y tribunales competentes.

3.3. INDEMNIZABILIDAD DEL TEMOR

El concepto de daño indemnizable con arreglo al artículo 82 RGPD es muy amplio y cubre, de entrada, cualesquiera menoscabos patrimoniales o no patrimoniales sufridos efectivamente por una persona física a raíz de un comportamiento infractor de la normativa protectora de los datos personales⁴⁹. El TJUE ha restringido doblemente este alcance extenso. Primero, ha señalado que no puede predicarse un daño *per se* de una mera infracción normativa⁵⁰: la víctima habrá de acreditar el perjuicio efectivamente sufrido como un requisito diferente e independiente al de la prueba de la infracción normativa

ECLI:EU:C:2024:288, apdo. 36; y STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531, apdo. 46.

⁴⁹ Considerando 75 RGPD: «Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados».

⁵⁰ STJUE de 4 de mayo de 2023, asunto C-300/21, *UI v. Österreichische Post AG*, ECLI:EU:C:2023:370, apdo. 42; STJUE de 25 de enero de 2024, asunto C-687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72, apdo. 61; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 43; y STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT c. PS GbR y otros*, ECLI:EU:C:2024:536, apdo. 28.

cometida, sin que ello obste a que pueda contar con mecanismos procesales que contribuyan a la acreditación de aquel en el pleito. Y, segundo, también ha indicado el TJUE que no sucede un daño automáticamente por la infracción del derecho a la protección de datos o por la infracción de una norma del RGPD que atribuye un derecho o potestad a un individuo⁵¹. El daño es, pues, algo más que la mera vulneración de un derecho.

Una de las cuestiones más interesantes decididas por el TJUE se refiere a la indemnizabilidad del temor por un mal uso potencial de los datos personales de un sujeto. Pueden identificarse escenarios en los cuales, después de un hecho accidental que no genera perjuicios inmediatos, el impacto que experimentan los individuos queda reducido al miedo o la angustia de que en el futuro puedan sufrir un daño cierto. Por ejemplo, una brecha de seguridad en una base de datos y una pérdida de control sobre los mismos puede llevar a una persona a temer que finalmente aquellos se revelen a terceros o que se usen de forma ilícita. En el ámbito de la IA generativa pueden también identificarse supuestos de daños derivados de la mera exposición a un riesgo. Un ejemplo de ello sería el de la angustia generada por conocer que un modelo entrenado ilícitamente con los propios datos puede llegar a ser desarrollado con fines maliciosos o pueda llegar a producir *outputs* dañosos en el futuro. Obsérvese que la mera infracción inicial cometida por el desarrollador del modelo –por ejemplo, no contar con una base de licitud válida– es insuficiente por ella misma para generar responsabilidad civil y que es necesaria la acreditación de un daño real y efectivo. El mero entrenamiento de un modelo con datos personales no genera automáticamente un daño patrimonial u otro no patrimonial a todas las víctimas, pero, en aplicación de la jurisprudencia del TJUE, algunas de ellas, ante la posibilidad de que sus datos puedan llegar a ser afectados en el futuro, pueden haber experimentado una situación de miedo, angustia o desamparo tal que revele el sufrimiento real de un daño moral.

En el último de los asuntos sobre esta cuestión –la Sentencia de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*⁵²–, el TJUE se enfrentó a un supuesto de pérdida hipotética de control sobre unos datos personales. Los hechos del caso fueron los siguientes: dos clientes de una asesoría

⁵¹ STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 37. Sobre la compensación de una posible vulneración del derecho de acceso, pende actualmente un asunto ante el TJUE. Se trata del asunto C-526/24, derivado de la petición de decisión prejudicial formulada el 31 de julio de 2024 por el *Amtsgericht* Arnsberg (Tribunal de lo Civil y Penal de Arnsberg, Alemania), en un caso con las partes siguientes: *Brillen Rottler GmbH & Co c. KG*.

⁵² STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536. Para un comentario a la sentencia, véase Carrasco Perera, A. (Septiembre de 2024). El daño que consiste en no saber si se ha producido o no una infracción y un perjuicio de datos personales. *GA-P Análisis*. <https://ga-p.com/publicaciones/el-dano-que-consiste-en-no-saber-si-se-ha-producido-o-no-una-infraccion-y-un-perjuicio-de-datos-personales/>.

fiscal en Alemania informaron a sus empleados de un cambio de dirección postal, que fue correctamente modificado en sus bases de datos. A pesar de haber recibido varios correos en el nuevo domicilio, la carta con las declaraciones fiscales del año 2019 fue enviada al domicilio anterior, cuyos nuevos residentes abrieron por error y, finalmente, entregaron a unos allegados de los demandantes. No se sabe del cierto y no se pudo acreditar en el pleito que en el sobre abierto figurara, además de la declaración, documentación adicional con datos personales de los actores tales como fechas de nacimiento, datos de los hijos, profesiones y lugares de trabajo, pertenencia a una comunidad religiosa o la condición de persona con discapacidad de un miembro de su familia.

Los clientes demandaron a la asesoría fiscal y solicitaron una indemnización de 15000 euros por el daño moral sufrido a consecuencia de la divulgación de sus datos personales a terceros. El Tribunal de lo Civil y Penal de Wesel (*Amtsgericht* Wesel) decidió suspender el procedimiento y plantear varias cuestiones prejudiciales al TJUE. Entre ellas, inquirió acerca de «si el temor a que los datos personales lleguen a manos de personas no autorizadas puede constituir, por sí solo, un daño inmaterial capaz de generar un derecho a una indemnización pecuniaria en virtud del artículo 82 del RGPD»⁵³.

El TJUE señala que «[l]a pérdida de control sobre los datos personales, incluso durante un breve período de tiempo, puede causar al interesado “daños y perjuicios inmateriales” [...] que den lugar a un derecho a indemnización, siempre que dicho interesado demuestre que ha sufrido efectivamente tales daños y perjuicios, por mínimos que sean»⁵⁴; y que no basta simplemente con alegar el temor para acreditar el daño efectivamente sufrido⁵⁵.

Con anterioridad, el TJUE ya se había pronunciado en dos ocasiones acerca de la indemnizabilidad del temor. En el primero de los casos –el asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*⁵⁶ –, el miedo a indemnizar se producía a consecuencia de un ataque informático por un *hacker* que había comprometido la seguridad de una base de datos dependiente del Ministerio búlgaro de finanzas y se había hecho con datos personales de millones de ciudadanos: cientos de ellos entablaron acciones para ser compensados por la angustia de saber que sus datos podían llegar a ser utilizados con fines maliciosos en el futuro. En el segundo de los casos –el asunto C-687/21, *BL c.*

⁵³ Apdo. 15.

⁵⁴ Apdo. 33.

⁵⁵ Apdo. 35.

⁵⁶ STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986.

*MediaMarktSaturn*⁵⁷–, el TJUE hubo de enfrentarse con las bases sentadas en el caso anterior a una demanda que es punto menos que un despropósito: el actor acudió a un centro comercial donde compró un electrodoméstico, que había de recoger luego en un mostrador al efecto. Otro cliente acudió al mostrador y recogió por error el electrodoméstico comprado por el primero de ellos, junto con el contrato y demás documentación que incluía datos personales de este, tales como su nombre, teléfono y dirección postal. En una media hora se pudo recuperar el electrodoméstico y la documentación, y era muy probablemente que el segundo cliente no hubiera tenido acceso efectivo a los datos. A pesar de ello y aunque el vendedor se había ofrecido a entregar el aparato sin coste en su domicilio, el afectado formuló demanda y exigió una indemnización por el daño moral resultante de la exposición al riesgo de que su información hubiera podido llegar a ser conocida por terceros o copiada y utilizada más adelante. El TJUE recuerda que las sensaciones de temor ante el riesgo de una futura utilización de los datos pueden constituir daños no patrimoniales, pero que incumbe al afectado acreditar su concurrencia. Además, el Tribunal indica que «[...] *el riesgo puramente hipotético de un uso indebido por parte de un tercero no autorizado no puede dar lugar a indemnización alguna. Ello será el caso cuando ningún tercero hubiera tenido conocimiento de los datos personales en cuestión*»⁵⁸.

Los tres casos resueltos por el TJUE hasta la fecha acerca de la indemnización del temor sufrido por experimentar el riesgo de un daño futuro derivado de la potencial utilización maliciosa de los datos personales propios invitan a formular varias cuestiones, que podrán llegar a plantearse en los años próximos en las controversias que surjan en el campo de la IA generativa.

La primera de ellas se refiere a la identificación del riesgo frente al que se experimenta el temor. El Tribunal únicamente ha señalado que el riesgo puramente hipotético no puede justificar una indemnización por el temor sufrido. Por lo tanto, a efectos de la pretensión indemnizatoria, será necesario identificar un riesgo real. En otros términos, será necesario establecer que algún tercero o grupo de terceros ha obtenido conocimiento de los datos personales en cuestión, pues sin tal conocimiento el riesgo es meramente hipotético. Hay varias críticas que pueden formularse a esta apreciación que hace la jurisprudencia del TJUE: (i) Uno puede experimentar el temor con independencia de si el riesgo es real o inexistente o hipotético: un sujeto puede sufrir miedo y ansiedad si efectivamente conoce que terceros han tenido acceso a sus datos o si cree que ello es posible pero lo ignora. Saber *ex post* que nadie tuvo acce-

⁵⁷ STJUE de 25 de enero de 2024, asunto C-687/21, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72.

⁵⁸ Apdo. 68 (traducción del autor: la STJUE no está disponible en español).

so a los datos puede poner punto final al temor, pero no elimina que en un periodo más o menos largo de tiempo aquel individuo habrá experimentado el temor. Acaso el Tribunal podría clarificar que, en este último supuesto, el temor constituye un riesgo general de la vida o un daño que el afectado tiene el deber jurídico de soportar; (ii) Señala el TJUE que no procede la compensación del temor cuando ningún tercero hubiera tenido conocimiento de los datos personales, pero no aclara qué ha de entenderse por «conocimiento». En particular, desconocemos si ha de tratarse de un conocimiento efectivo, que puede resultar muy difícil de acreditar por la víctima, o de una posibilidad razonable de conocer los datos; y (iii) el TJUE no parece distinguir los tres casos resueltos hasta la fecha sobre indemnizabilidad del temor y ofrece una solución común a todos ellos, cuando hay un factor que puede convertir el riesgo en cuestión en jurídicamente relevante: un comportamiento doloso o intencional que incrementa irrazonablemente el riesgo de un mal uso frente a un descuido o a un error que resulta únicamente en un potencial acceso inadecuado a los datos pero que no parece contribuir a un incremento irrazonable del riesgo. No parece que todos estos casos hayan de recibir el mismo tratamiento jurídico.

La segunda cuestión que plantea la jurisprudencia del TJUE hace referencia al umbral de dolor o de temor requerido para fundar un derecho a ser compensado. Si el temor es el daño moral indemnizable, el TJUE recuerda que no puede aplicarse una regla *de minimis* y que cualquier daño, por pequeño que sea, puede ser objeto de compensación. La víctima deberá acreditar la realidad de este dolor, sin que baste la mera alegación de haberlo experimentado. La víctima deberá pues aportar elementos de prueba suficiente para acreditar haber sufrido este temor⁵⁹. Un problema con este tipo de daño inmaterial deriva del hecho que las personas experimentamos el miedo y el temor de modos diferentes: hay personas más aprehensivas que otras y personas más tolerantes del dolor. El temor es pues, en buena medida, un daño idiosincrático. Por ello, la prueba dependerá de factores externos y objetivos. Si no hay documentos o testigos que acrediten la realidad del dolor, el principal elemento de prueba acabará siendo la gravedad de los hechos e inferir el daño *in re ipsa*. En consecuencia, de algún modo, no se acabarán indemnizando las situaciones menos graves: una regla *de minimis* se acabará aplicando por la puerta de atrás.

⁵⁹ STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986: «[...] cuando una persona que solicita una indemnización por este motivo invoca el temor de que en el futuro se produzca un uso indebido de sus datos personales como consecuencia de dicha infracción, el órgano jurisdiccional que conozca del asunto deberá comprobar que ese temor puede considerarse fundado, habida cuenta de las circunstancias específicas del caso y del interesado» (apdo. 85).

La tercera cuestión acerca de esta línea jurisprudencial del TJUE se refiere a las consecuencias que ha de desplegar la concreción futura del riesgo, esto es, de la materialización de un daño a resultas del uso ilícito de los datos personales por un tercero en un momento más o menos alejado en el tiempo. En otros términos, el temor que padecía la víctima a que sus datos se utilizaran se convierte en realidad y estos finalmente son divulgados, utilizados para obtener determinados beneficios, manipulados o de algún otro modo empleados por un tercero. Con arreglo a la jurisprudencia del TJUE, hay que distinguir dos tipos de daños en estas situaciones: el temor experimentado efectivamente por la víctima y el daño resultante del mal uso posterior de los datos (que podrá ser patrimonial o no patrimonial)⁶⁰. En otras palabras, el TJUE permite la indemnización del temor como tal, pero no se refiere a la compensación de un daño probabilístico, definido como el daño futuro causado por el tercero multiplicado por la probabilidad de que ocurra. Son pues dos daños diferentes causados por hechos y sujetos diferentes. El Prof. Ángel Carrasco ha explicado que el TJUE admite la indemnización del temor porque ya hay daño pero que no se refiere a la indemnizabilidad de un daño temido, para el cual el derecho en ocasiones «ha previsto una especie de *cautio damni infecti* mediante la que el juez ordena al demandado (si así se aprecia) prestar una caución»⁶¹. Al tratarse de daños diferentes, una vez materializado el riesgo, el responsable del tratamiento demandado que satisfizo la indemnización a la víctima no ostentará ningún derecho de repetición o reembolso contra quien hubiera después usado ilícitamente los datos personales.

3.4. BRECHAS DE SEGURIDAD

Los modelos de lenguaje extenso y, por ello, los modelos de IA generativa pueden ser objeto de varias acciones maliciosas que comprometan su ciberseguridad⁶². En primer lugar, pueden destacarse los *privacy attacks* o *information*

⁶⁰ Por ejemplo, en el asunto *Scalable Capital*, el TJUE distingue dos tipos de perjuicios diferentes: el posible daño directo derivado de una pérdida de datos a partir de un ciberataque y el posible daño futuro derivado de una usurpación o fraude de identidad. En el caso, terceros no identificados accedieron maliciosamente a datos personales y otros relacionados con el funcionamiento de una *trading app* o aplicación informática de negociación con valores, gestionada por la sociedad alemana Scalable Capital. Véase STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531, apdos. 54-58.

⁶¹ Carrasco Perera, A. (Septiembre de 2024). *Op. cit.*, pág. 4.

⁶² Para una descripción general de los diferentes riesgos asociados a la seguridad de la información en el campo de la IA generativa, véase Bundesamtes für Sicherheit in der Informationstechnik (Abril de 2024). Generative AI Models Opportunities and Risks for Industry and Authorities. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4.

extraction attacks: su objetivo es obtener información acerca de la arquitectura de un modelo para reconstruirlo totalmente o en parte o conseguir información sobre los datos utilizados en su entrenamiento. Ello puede realizarse, por ejemplo, mediante consultas acerca de si determinada información fue utilizada o no (*membership inference attacks*) o por medio de otros *prompts*. A partir de diferentes técnicas, un tercero puede llegar a obtener datos personales que fueron utilizados en el entrenamiento de un modelo, datos personales añadidos como *inputs* por un usuario durante su utilización de un sistema de IA generativa, y también datos personales contenidos en las generaciones o *outputs* producidos por el sistema. Por otra parte, hay riesgos de reidentificación de datos anonimizados.

La seguridad de un modelo o sistema de IA generativa también puede afectarse mediante *evasion attacks*, que persiguen alterar y manipular el comportamiento de aquellos o evadir medidas de protección adoptadas por sus desarrolladores. Así, pues, es posible que un tercero mediante determinadas técnicas pueda eludir los diferentes filtros y mecanismos de protección implementados para que un sistema no produzca determinados resultados. En otros términos, aunque el desarrollador de un sistema de IA generativa hubiera adoptado filtros para que determinados datos personales sensibles no pudieran ser revelados por medio de *outputs*, un tercero sofisticado podría llegar a sortear tales barreras y obtener los datos en cuestión. Entre las técnicas utilizables, destacan las llamadas *prompt injections*.

Otro grupo de problemas de ciberseguridad tiene que ver con los denominados *poisoning attacks*. Se trata de acciones que persiguen alterar o manipular características del modelo como los datos de entrenamiento o su propia arquitectura. En el primer caso, si se anticipa que un modelo puede entrenarse con determinadas fuentes, el «envenenamiento» pasa, por ejemplo, por una manipulación de las páginas web que se rastrean para generar la base de datos. En el segundo caso, ello puede ser más factible en casos de modelos licenciados en abierto –cuyos pesos y variables pueden ser públicos–, que pueden ser desarrollados luego por cualquier tercero y que pueden dar lugar a alteraciones maliciosas de su estructura y características.

Dados los riesgos descritos, es probable que individuos que conozcan que un determinado modelo o sistema de IA generativa ha sido objeto de un ataque que haya permitido un acceso a sus datos personales o una manipulación o alteración de estos resuelvan emprender acciones de responsabilidad civil contra el titular o desarrollador de aquel. Obsérvese que se trata de comportamientos llevados a cabo por terceros difícilmente identificables y que actúan dolosamente y, por tanto, puede plantearse la conveniencia de imputar tales daños al demandado. En otros términos, se abre la vía a acudir a criterios

de imputación objetiva para desligar o no al demandado de las pretensiones indemnizatorias o, desde una perspectiva tradicional, para identificar una interrupción del nexo causal. De hecho, el propio artículo 82.3 RGPD establece que «[e]l responsable o encargado del tratamiento estará exento de responsabilidad [...] si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios». No obstante, en aplicación de este precepto, puede sostenerse que el titular o desarrollador del modelo o sistema de IA generativa puede llegar a responder si no hubieran adoptado las medidas técnicas adecuadas de seguridad de la información que hubieran evitado el ataque o al menos mitigado de forma razonable su ocurrencia. Esto es, puede llegar a responder si su omisión o la adopción de medidas insuficientes ha contribuido irrazonablemente a un incremento del riesgo de ciberataque.

En relación con esta cuestión, se ha pronunciado ya el TJUE en una sentencia ya citada: la STJUE de 14 de diciembre de 2023 dictada en el asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*⁶³. El caso se refería al acceso malicioso por un tercero a datos de millones de ciudadanos búlgaros que se contenían en una base gestionada por una agencia pública, dependiente del Ministerio de Finanzas, encargada de identificar y reclamar deudas públicas. Parte de esta información fue publicada luego en internet.

Cientos de ciudadanos demandaron a la agencia *Natsionalna agentsia za prihodite* (en adelante, NAP), entre ellos, la actora en el pleito del que finalmente tuvo conocimiento el TJUE. En su reclamación ante los tribunales búlgaros, la Sra. VB solicitó la cantidad de 1000 leva (aproximadamente, unos 510 euros) por el daño moral consistente en que alguien pudiera utilizar la información publicada en internet o que, gracias a ella, pudieran chantajearla, atacarla o secuestrarla.

La principal defensa de NAP consistió en afirmar que había adoptado todas las medidas técnicas necesarias *ex ante* para evitar un ciberataque como el efectivamente sufrido y *ex post* para mitigar las consecuencias negativas de este. Para el TJUE, el examen de si un responsable del tratamiento ha cumplido con sus obligaciones de seguridad con arreglo a los artículos 24.1 y 32 RGPD ha de hacerse caso por caso. Es necesario que los tribunales que decidan acerca de una pretensión indemnizatoria por los daños derivados de una brecha de seguridad aprecien si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento fueron apropiadas, teniendo en cuenta los riesgos vinculados al tratamiento y apreciando si la naturaleza, el contenido

⁶³ STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986. Para un comentario de la Sentencia, véase Martín Faba, J. M. (2024). Novedades en materia de indemnización y protección de datos personales. *Revista CESCO De Derecho De Consumo*, (49), 131-147. https://doi.org/10.18239/RCDC_2024.49.3474.

y la adopción de esas medidas están adaptados a estos riesgos y, por lo tanto, que examinen si hubo o no una infracción del RGPD⁶⁴. Para el Tribunal, incumbe al responsable del tratamiento demandado en el proceso la carga de la prueba de acreditar que las medidas técnicas y organizativas adoptadas fueron apropiadas y que, en efecto no infringió el RGPD⁶⁵. Ello deriva del principio de responsabilidad activa previsto en el artículo 5.2 RGPD que establece el deber de los responsables del tratamiento de demostrar que cumplen con lo previsto en el Reglamento. Aclara también el Tribunal que confiar la acreditación del carácter apropiado o inapropiado de las medidas técnicas y organizativas solo y exclusivamente a un informe pericial es contrario al principio de efectividad del derecho de la UE: un informe pericial presentado de parte o solicitado por un juez puede ser una prueba relevante, pero no siempre será necesaria y sus conclusiones pueden ser contradichas por otros tipos de pruebas⁶⁶. Finalmente, destaca el TJUE, que, si las medidas resultan inapropiadas, ya no es posible para el responsable del tratamiento exonerarse de responder conforme a lo previsto en el artículo 82.3 RGPD: ya no es «*en modo alguno responsable del hecho que haya causado los daños y perjuicios*», por cuanto su comportamiento contribuyó, en menor o mayor grado, a la producción de los daños.

En suma, en los pleitos de responsabilidad civil por daños derivados de problemas de seguridad de la información relacionados con la IA generativa, de seguirse esta línea jurisprudencial, se produciría una inversión de la carga de la prueba en relación con la acreditación de uno de los requisitos de la pretensión: corresponderá al responsable demandado probar que no infringió el artículo 32 RGPD y que las medidas técnicas y organizativas adoptadas para reducir o eliminar los riesgos asociados con la ciberseguridad fueron apropiadas. Por su parte, incumbirá al actor en el pleito la prueba del daño efectivamente sufrido y de la relación de causalidad.

3.5. RELACIONES CON OTROS FUNDAMENTOS DE RESPONSABILIDAD: EL CASO DE LOS DEEPFAKES

Un supuesto específico de causación de daños en el campo de la IA generativa resultará de la generación y uso posterior de ultrasuplantaciones o *deepfakes*. Por ejemplo, un usuario puede utilizar un sistema de IA generativa

⁶⁴ Apdo. 47. El TJUE no valora la posibilidad de que la infracción normativa hubiera podido ser identificada y, en su caso, sancionada por una agencia de protección de datos y que papel tendría esta resolución en el pleito civil de reclamación de daños y perjuicios. En consecuencia, a falta de un procedimiento administrativo previo o en paralelo, la prueba de la infracción habrá de establecerse en el pleito civil (*stant-alone claims*).

⁶⁵ Apdo. 57.

⁶⁶ Apdo. 64.

para generar y luego divulgar un vídeo sintético que muestre a un individuo tomando parte en unos hechos en los cuales nunca participó o diciendo unas palabras que nunca pronunció.

Una de las cuestiones principales que se plantea en este caso –además de la posibilidad de reclamar frente al operador del sistema, por ejemplo, si el usuario que divulgó el vídeo no puede ser identificado– es el de si la víctima puede acudir a otras bases diferentes del artículo 82 RGPD para fundar su pretensión indemnizatoria. En particular, en el derecho español, se pueden señalar al menos tres fundamentos diferentes que, en función de los casos podrán llegar a alegarse: la responsabilidad civil extracontractual general recogida en los artículos 1902 y ss. CC; la responsabilidad civil derivada de delito prevista en los artículos 109-122 CP; y la responsabilidad civil por intromisiones ilegítimas en los derechos al honor, propia imagen e intimidad personal y familiar regulada en la LO 1/1982⁶⁷. Seguramente, los actos de producción, comunicación y difusión del vídeo constituirán, a falta de una causa de exoneración, intromisiones ilegítimas en el derecho a la propia imagen de la persona cuya imagen se ha reproducido sintéticamente; además, en función del contenido del vídeo, podrán vulnerarse sus derechos al honor y a la intimidad personal; y, finalmente, puesto que para la generación del vídeo se habrán tratado datos personales de la persona afectada en varios momentos, es también posible que se hayan cometido infracciones del RGPD que lleven aparejadas la causación de un daño moral a aquella compensable con arreglo al artículo 82 RGPD.

La acción prevista en el artículo 82 RGPD es acumulable a otras acciones indemnizatorias. En este sentido, el considerando 146 RGPD señala que el régimen que prevé para la compensación de los daños y perjuicios derivados de un tratamiento de datos personales en infracción de la normativa ha de entenderse «*sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros*»⁶⁸. Acudir al artículo 9.3 de la LO 1/1982 en lugar de a la acción prevista en el artículo 82 RGPD puede resultar atractivo para las víctimas en estos

⁶⁷ Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115, de 14.5.1982).

⁶⁸ Sobre la compatibilidad de diferentes pretensiones indemnizatorias en el ámbito de la protección de datos personales, véanse Moreno Martínez, J.A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. Ataz López, J. y Cobacho Gómez, J.A. (Coords.) (2021). *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*. Thomson -Aranzadi, Tomo 3, 515-565; y Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución*, 34, 197-232.

casos: el precepto establece una presunción de causación de daño moral a partir de la intromisión ilegítima en uno de los derechos de la personalidad protegidos por la ley; que, además, ha sido calificada en la jurisprudencia como una presunción *iuris et de iure* que no admite prueba en contrario. En efecto, la víctima fundando su pretensión indemnizatoria en la LO 1/1982 puede ahorrarse los esfuerzos necesarios para la acreditación del daño no patrimonial resultante de un *deepfake*, que de acudir al remedio del artículo 82 RGPD habría de realizar.

Sea como fuere, surgen dos problemas que podrán llegar a discutirse en los litigios planteados en relación con la IA generativa. El primero de ellos se refiere a la posibilidad de acumulación de acciones y de obtención de indemnizaciones supracompensatorias. El TJUE ha señalado que el derecho interno puede contar con normas que permitan fijar una indemnización superior a la reparación total y efectiva de los daños cubierta por el artículo 82 RGPD⁶⁹: : «[...] si el Derecho nacional lo permite, el juez nacional pued[e] conceder al interesado una indemnización superior a la reparación total y efectiva prevista en el artículo 82, apartado 1, del RGPD en caso de que, habida cuenta de que el perjuicio también ha sido causado por la infracción de disposiciones de Derecho nacional [...], esta última reparación no se considere suficiente o adecuada». En buena medida, la cuestión pasará por determinar si las normas nacionales infringidas son normas de desarrollo del RGPD o no. En el primer supuesto, la indemnización no podrá superar el principio de reparación integral del que parte el RGPD: el máximo indemnizable es el perjuicio efectivamente sufrido por la víctima y no podrán tenerse en cuenta la infracción simultánea de varias disposiciones internas para incrementar el *quantum* indemnizatorio⁷⁰. En el segundo supuesto, parece que el TJUE admite la acumulación de diferentes pretensiones de daños y la posibilidad de obtener una indemnización superior⁷¹. Claramente, la acción prevista en el art. 9.3 LO 1/1982 no forma parte de una norma de desarrollo del RGPD. Un legislador nacional también podría aprobar una norma interna sobre *deepfakes* que incluyera normas sobre compensación de daños con criterios autónomos de cuantificación de daños. El segundo de los problemas afecta a la posibilidad de que la utilización de un remedio o fundamento diferente previsto en el derecho interno de un Estado miembro llegue a transgredir los principios de efectividad y equivalencia del Derecho de la UE. Habrá que examinar hasta qué punto disposiciones internas que establecen reglas diferentes

⁶⁹ STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536, apdo. 49.

⁷⁰ STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536, apdos. 48 y 50.

⁷¹ En el asunto *PS*, las normas supuestamente infringidas que daban lugar a compensación formaban parte de las regulaciones sobre la profesión de asesor fiscal.

de compensación de los daños en supuestos en los cuales hay un tratamiento de daños personales pueden llegar a menoscabar la efectividad del remedio indemnizatorio establecido en el Reglamento.

3.6. PLURALIDAD DE SUJETOS RESPONSABLES

La cadena de valor o ciclo de vida de la IA generativa implica diferentes estadios o tareas que pueden ser llevados a cabo por sujetos diferentes. No necesariamente el desarrollador de un modelo de IA generativa habrá elaborado él mismo las bases de datos utilizadas en su entrenamiento; puede encargar a un tercero que lleve a cabo tareas de *fine-tuning*, o puede licenciar el modelo a terceros para que sean estos quienes desarrollen sistemas o integren el modelo en sus propios servicios. La pluralidad de sujetos requerirá la identificación de los diferentes roles que hayan de corresponder a cada uno y el cumplimiento de los deberes establecidos en el RGPD para la distribución de responsabilidades. En particular, para cada operación de tratamiento o conjunto de tratamientos relacionados deberá examinarse qué sujeto o sujetos asumen la posición de responsable o corresponsables; y, en su caso, si otros actúan como encargados del tratamiento. La delimitación de las diferentes posiciones no siempre es sencilla, especialmente, por el concepto de corresponsabilidad en el tratamiento de datos personales que ha desarrollado el TJUE⁷².

El artículo 26.1. RGPD señala que «cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento [...]». Para que haya corresponsabilidad, los diferentes sujetos han de poder ser considerados a título individual responsables del tratamiento *ex* artículo 4.7 RGPD, esto es, ambos han de haber influido efectivamente en la determinación de los fines y medios del tratamiento. Y, por otro lado, han de tener alguna relación entre ellos, puesto que su influencia en la determinación de los fines y medios debe ejercerse conjuntamente⁷³.

⁷² En este sentido, véanse STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH /Facebook Ireland Ltd/Votreter des Bundesinteresses beim Bundesverwaltungsgericht*. ECLI:EU:C:2018:388; STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyyskunta*. ECLI:EU:C:2018:551; STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629; y STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcijak*. ECLI:EU:C:2023:949.

⁷³ Sobre los diferentes criterios exigidos, véase Rubí Puig, A. (2024). El principio de culpabilidad en el derecho de protección de datos personales y la condición de responsable del tratamiento. *La Ley Unión Europea*, 121, 1-16.

La participación conjunta en la determinación de los fines y medios que genera la situación de corresponsabilidad en el tratamiento puede llevarse a cabo de maneras diversas: (i) un acuerdo o decisión común por dos o más personas; o (ii) una convergencia en las decisiones efectuadas independientemente, que se complementan para influir decisivamente en la determinación de los fines y medios. Sea como sea, no es necesario un acuerdo formal entre los implicados en las operaciones de tratamiento de datos personales para que surja una situación de corresponsabilidad. El TJUE patrocina una visión funcional y no formalista del derecho de protección de datos personales, que implica la necesidad de evaluar todas las circunstancias fácticas de cada caso para la asignación de roles y distribuciones de responsabilidades.

El TJUE ha resuelto que una situación de corresponsabilidad no exige una responsabilidad equivalente. Los diferentes corresponsables pueden estar implicados en diferentes etapas del tratamiento de los datos personales, pueden participar en diferentes grados o pueden obtener resultados diversos⁷⁴. El TJUE también ha venido afirmando que, para darse una situación de corresponsabilidad, no es necesario que todos los corresponsables tengan acceso a los datos personales tratados⁷⁵.

Desde el punto de vista de la reparación de los daños, el artículo 82 RGPD también establece una serie de reglas que podrán jugar un papel importante en los pleitos contra diferentes agentes en la cadena de valor de la IA generativa, como potenciales responsables civiles.

En primer lugar, se establece una regla de solidaridad en el artículo 82.4 RGPD. Así, en caso de pluralidad de corresponsables, en supuestos de concurrencia de un responsable y un encargado del tratamiento o en otras situaciones de pluralidad subjetiva, *«cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado»*⁷⁶. En segundo lugar, en la relación interna de solidaridad se prevé

⁷⁴ Véase Comité Europeo de Protección de Datos (7 de julio de 2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*. https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf, pp. 22-23.

⁷⁵ Véase, especialmente, STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629.

⁷⁶ Con arreglo al considerando 146 RGPD, un legislador interno puede decidir prescindir del carácter solidario de la obligación de reparar los daños y transformarla en una regla parciaria, siempre que se salguarde el derecho del interesado a recibir una indemnización total y efectivo. El legislador español ha optado por una regla de solidaridad. En este sentido, véase artículo 30.2. de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE nú., 294 de 6.12.2018): *«Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados»*.

una acción de repetición o regreso para aquel demandado que haya satisfecho la indemnización total al perjudicado. Conforme al artículo 82.5 RGPD, este podrá «*reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados*». De seguro, la implicación de varios agentes en la cadena de valor de la IA generativa va a ofrecer un buen campo de pruebas para examinar el funcionamiento de estas reglas en los futuros pleitos de responsabilidad civil por infracciones normativas del derecho de protección de datos personales.

4. CONCLUSIONES

El desarrollo y funcionamiento de modelos y sistemas de IA generativa conllevarán con frecuencia tratamientos de datos personales y, en efecto, incumbirá a sus desarrolladores y operadores cumplir con los principios y obligaciones establecidas en el RGPD y demás normativa protectora del derecho a la protección de los datos de carácter personal. En estos momentos, son muchas las cuestiones abiertas acerca de cómo ha de cumplirse con lo establecido en el RGPD –por ejemplo, hay dudas acerca de las bases de licitud que puedan amparar la compilación de bases de datos o el entrenamiento de modelos de IA generativa; acerca del nivel de medidas técnicas y organizativas exigibles; o acerca de la relación entre diferentes agentes en la cadena de valor de la IA generativa. Los rasgos generales de la IA generativa –gran tamaño, generalidad y opacidad– contribuyen a este nivel de incertidumbre, pero es esperable que en los próximos años agencias de protección de datos y tribunales vayan de modo progresivo ofreciendo respuestas y consolidando un marco legal de aplicación a los tratamientos de datos personales realizados en este ámbito. A pesar de la incertidumbre actual o acaso a consecuencia suya, es probable que algunos desarrolladores y operadores en la cadena de valor de la IA generativa hayan infringido ya o lleguen a infringir disposiciones del RGPD y, a resultas, hayan causado o causen daños y perjuicios a personas físicas.

Es probable también que algunas de estas personas entablarán acciones de responsabilidad civil para resarcirse de los daños sufridos como consecuencia del desarrollo y funcionamiento de herramientas de IA generativa. Cuando los daños y perjuicios sean de los que el RGPD persigue prevenir y compensar, el artículo 82 RGPD ofrecerá un buen fundamento para la responsabilidad civil de responsables y encargados de los tratamientos de datos personales en la cadena de valor de la IA generativa. Los litigios que se lleguen a plantear en este sector ofrecerán un campo de pruebas para examinar si la jurisprudencia

elaborada por el TJUE en interpretación de este precepto es adecuada o no para la IA generativa. Es probable que, en estos asuntos, se lleguen a examinar los problemas que han sido apuntados en este trabajo, tales como las consecuencias de reparar daños de bagatela y de fijar indemnizaciones simbólicas; la indemnizabilidad del temor a que los datos personales propios puedan ser utilizados ilícitamente en el futuro; la imputación subjetiva y objetiva de los daños derivados de incidencias en la seguridad de la información de modelos y sistemas de IA generativa; la compatibilidad del remedio previsto en el artículo 82 RGPD con otros fundamentos de responsabilidad civil; y la adecuación de una regla de solidaridad en la obligación de responder de varios sujetos implicados en la cadena de valor de la IA generativa.

BIBLIOGRAFÍA UTILIZADA

A) LITERATURA ACADÉMICA

- Achille, A., Kearns, M., Klingenberg, C., y Soatto, S.O. (2023). AI model disgorgement: Methods and choices. *Proceedings of the National Academy of Sciences of the United States of America*, 121 (<https://doi.org/10.48550/arXiv.2304.03545>).
- Arroyo i Amayuelas, E. (2024). El scoring de Schufa. *InDret* 3.2024. 134-160.
- Beckers, A., y Teubner, G. (2021). *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds*. Hart, 161-162.
- Brown, H., Lee, K., Mireshghallah, F., Shokri, R., y Tramèr, F. (2022). What Does It Mean for a Language Model to Preserve Privacy?. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 2280–92. <https://doi.org/10.1145/3531146.3534642>.
- Carlini, N., Tramer, F., Wallace, E., Jagielski, M. et al. (2021). Extracting Training Data from Large Language Models. *30th USENIX Security Symposium*. <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>. 2633-2650.
- Carlini, N., Hayes, J., Nasr, M., Jagielski, M., Sehwag, V., Tramèr, F., Balle, B., Ippolito, D., y Wallace, E. (2023). Extracting Training Data from Diffusion Models. *ArXiv, abs/2301.13188*.
- Carrasco Perera, A. (Septiembre de 2024). El daño que consiste en no saber si se ha producido o no una infracción y un perjuicio de datos personales. *GA-P Análisis*. <https://ga-p.com/publicaciones/el-dano-que-consiste-en-no-saber-si-se-ha-producido-o-no-una-infraccion-y-un-perjuicio-de-datos-personales/>.

- Carrière-Swallow, Y., y Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective. *IMF Departmental Papers* 19 (16), 2019. 1-46.
- Chang, C. (2024). When AI Remembers Too Much: Reinventing The Right To Be Forgotten For The Generative Age. *Washington Journal of Law and Technology and the Arts*, 19(3) 22-45.
- Chiara, P.G. (2023). Italy: Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing. *European Data Protection Law Review*. Vol. 9. 68–72.
- Davara Rodríguez, M.A. (2021). Tratamiento (Comentario al Artículo 4.2 RGPD). Troncoso Reigada A. (Dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. Tomo I, Thomson Reuters –Civitas. 591-628.
- El-Mhamdi, E., Farhadkhani, S., Guerraoui, R., Gupta, N., Hoang, L.N., Pinot, R., y Stephan, J. (2022). On the Impossible Safety of Large AI Models. *ArXiv, abs/2209.15259*.
- Famularo, J. (2023). Platform-Related Harms., *Yale-Wikimedia Initiative on Intermediaries & Information*, 1-14. https://law.yale.edu/sites/default/files/area/center/isp/documents/platformrelatedharms_ispessayseries_2023.pdf. Págs. 8-9.
- Gil González, E. (2022). *El interés legítimo en tratamientos de datos personales*. La Ley.
- Guadamuz, A. (2024). A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs. *GRUR International*, 73(2), 111-127.
- Gupta, M., Akiri, C., Aryal, K., Parker, E., y Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, 11, 80218-80245.
- Hacker, P. (2021). A legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, 13(2), 257–301. <https://doi.org/10.1080/17579961.2021.1977219>.
- Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., y Liang, P. (2023). Foundation Models and Fair Use. *Stanford Law and Economics Olin Working Paper* No. 584. <https://ssrn.com/abstract=4404340>.
- Hine, E., Novelli, C., Taddeo, M., y Floridi, L. (2023). Supporting Trustworthy AI Through Machine Unlearning. *SSRN Scholarly Paper*. <https://doi.org/10.2139/ssrn.4643518>.
- Kretschmer, M., Margoni, T. y Oruç, P. (2024). Copyright Law and the Lifecycle of Machine Learning Models. *IIC*. vol. 55. 110-138.
- Lee, K., Cooper, F., y Grimmelmann, J. (2024). Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain. *Journal of the Copyright Society*, 2024. 1-128 (en prensa) (disponible a <http://dx.doi.org/10.2139/ssrn.4523551>).
- Marcos, H., y Pullin, M. (Octubre 2023). Large Language Models and EU Data Protection: Mapping (Some) of the Problems. *The Digital Constitutionalist*. ht-

- [tps://digi-con.org/large-language-models-and-eu-data-protection-mapping-some-of-the-problems](https://digi-con.org/large-language-models-and-eu-data-protection-mapping-some-of-the-problems).
- Martín Faba, J. M. (2024). Novedades en materia de indemnización y protección de datos personales. *Revista CESCO De Derecho De Consumo*, (49), 131–147. https://doi.org/10.18239/RCDC_2024.49.3474.
- Moreno Martínez, J.A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. Ataz López, J. y Cobacho Gómez, J.A. (Coords.) (2021). *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*. Thomson -Aranzadi, Tomo 3, 515-565.
- Mühlhoff, R., y Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology*, 16(1), 261–292. <https://doi.org/10.1080/17579961.2024.2313794>.
- Necati Pehlivan, C. (19 de septiembre de 2024). Inteligencia artificial y protección de datos. *Almacén de Derecho*. <https://almacenederecho.org/inteligencia-artificial-y-proteccion-de-datos>.
- Novelli, C., Casolari, F., Hacker, P., Spedicato, G., y Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *ArXiv*, *abs/2401.07348*. 1-36.
- Nunez Duffourc, M., Gerke, S., y Kollnig, K. (2024). Privacy of Personal Data In The Generative AI Data Lifecycle. *New York University Journal of Intellectual Property And Entertainment Law*. Vol. 13, n. 2. 219-268.
- Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, 5(4), 53-87.
- Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución*, 34, 197-232.
- Rubí Puig, A. (2024). El principio de culpabilidad en el derecho de protección de datos personales y la condición de responsable del tratamiento. *La Ley Unión Europea*, 121, 1-16.
- Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Álvarez Lata, N. (2024). *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*. APPDC-Aranzadi. 621-688.
- Ruscheimer, H. (2024). Generative AI and Data Protection. Calo, R., Ebers, M., Poncibò, C., y Zou, M. (2024). *Handbook on Generative AI and the Law*, Cambridge University Press (en prensa) (disponible en SSRN: <https://ssrn.com/abstract=4814999>).
- Staab, R., Vero, M., Balunović, M. y Vechev, M. (2023). Beyond Memorization: Violating Privacy Via Inference with Large Language Models. <https://arxiv.org/abs/2310.07298>.

- Varoquaux, G., Luccioni, A.S., y Whittaker, M. (2024). Hype, Sustainability, and the Price of the Bigger-is-Better Paradigm in AI. (<https://doi.org/10.48550/arXiv.2409.14160>).
- Zanfir-Fortuna, G. (12 de septiembre de 2023). How Data Protection Authorities are De Facto Regulating Generative AI. *Future of Privacy Forum*. <https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/>.

B) GUÍAS E INFORMES

- AEPD (febrero de 2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. <https://www.aepd.es/guias/ade-cuacion-rgpd-ia.pdf>.
- Bundesamtes für Sicherheit in der Informationstechnik (Abril de 2024). Generative AI Models Opportunities and Risks for Industry and Authorities. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4.
- CNIL, “Les fiches pratiques sur l’IA”, 2024 (<https://www.cnil.fr/fr/les-fiches-pratiques-ia>).
- Comité Europeo de Protección de Datos (7 de julio de 2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*. https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf.
- Confederation of European Data Protection Organisations (16 de octubre de 2023). Generative AI: The Data Protection Implications. *CEDPO AI Working Group*. <https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf>.
- European Data Protection Supervisor (3 de junio de 2024). Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems. https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf.
- Garante per la Protezione dei Dati Personali (septiembre de 2023). Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale. <https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0>.
- Hamburg Commissioner for Data Protection and freedom of information (2024). Discussion Paper: Large Language Models and Personal Data. https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf.

JURISPRUDENCIA DEL TJUE

STJUE de 19 de octubre de 2016, asunto C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*. ECLI:EU:C:2016:779.

STJUE de 20 de diciembre de 2017, asunto C-434/16, *Peter Nowak c. Data Protection Commissioner*. ECLI:EU:C:2017:994.

STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH / Facebook Ireland Ltd/Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*. ECLI:EU:C:2018:388.

STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyskunta*. ECLI:EU:C:2018:551.

STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629.

STJUE de 24 de septiembre de 2019, asunto C-136/17, *GC y otros c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773.

STJUE de 17 de junio de 2021, asunto C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, ECLI:EU:C:2021:492.

STJUE de 24 febrero 2022, asunto C-175/20, *SS SIA c. Valsts ierņēmumu dienests*. ECLI:EU:C:2022:124.

STJUE de 1 de agosto de 2022, asunto C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601.

STJUE de 8 de diciembre de 2022, asunto C-180/21, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*. ECLI:EU:C:2022:967.

STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370.

STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537.

STJUE de 9 de noviembre de 2023, asunto C-319/22, *Gesamtverband Autoteile-Handel eV c. Scania CVAB*. ECLI:EU:C:2023:837.

STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcijak*. ECLI:EU:C:2023:949.

STJUE de 7 de diciembre de 2023, asunto C-634/21, *OQ c. Land Hessen y SCHUFA Holding AG*. ECLI:EU:C:2023:957.

STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986.

STJUE de 14 de diciembre de 2023, asunto C-456/22, *VX, AT c. Gemeinde Ummendorf*, ECLI:EU:C:2023:988.

STJUE de 25 de enero de 2024, asunto C-687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72.

STJUE de 7 de marzo de 2024, asunto C-604/22, *IAB Europe c. Gegevensbeschermingsautoriteit*. ECLI:EU:C:2024:214.

STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288.

STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531.

STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*, ECLI:EU:C:2024:536.

STJUE de 12 de septiembre de 2024, asuntos acumulados C-17/22 y C-18/22, *HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG c. Müller Rechtsanwaltsgesellschaft mbH y otros*, ECLI:EU:C:2024:738.

El seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial

ALBERTO J. TAPIA HERMIDA

Catedrático de Derecho Mercantil

Universidad Complutense de Madrid

Consejero Académico de Estudio Jurídico Sánchez Calero

Sumario: 1. INTRODUCCIÓN. 2. ANTECEDENTES. 2.1. La Resolución del Parlamento Europeo sobre un régimen de responsabilidad civil en materia de inteligencia artificial de 20 de octubre de 2020. 2.2. La Propuesta de Directiva sobre responsabilidad en materia de inteligencia artificial de 28 de septiembre de 2022. 3. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL. 4. LAS CARACTERÍSTICAS DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL. 4.1. Seguro voluntario. 4.2. Seguro de responsabilidad civil empresarial o profesional. 5. LAS PARTES. 5.1. El asegurador. 5.2. El tomador y el asegurado. Las pólizas colectivas. 6. EL RÉGIMEN DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL. 6.1. Seguro de régimen común o seguro por grandes riesgos. 6.2. Aplicación de la LCS. 6.3. Aplicación de la LOSSEAR. 7. LA DELIMITACIÓN SUSTANCIAL DEL RIESGO CUBIERTO POR REFERENCIA A LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL. 7.1. Definición general del riesgo cubierto. 7.2. Descripción específica de los riesgos excluidos de la cobertura. 8. LA DELIMITACIÓN TEMPORAL DEL RIESGO CUBIERTO POR REFERENCIA A LAS RECLAMACIONES PRESENTADAS CONTRA EL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO. LAS CLÁUSULAS “CLAIMS MADE”. 9. LA DEFENSA JURÍDICA DEL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO FRENTE A LA RECLAMACIÓN DEL USUARIO PERJUDICADO O DE SUS

HEREDEROS. 10. LA ACCIÓN DIRECTA DEL USUARIO DE UN SISTEMA DE INTELIGENCIA ARTIFICIAL PERJUDICADO O SUS HEREDEROS CONTRA EL ASEGURADOR DEL OPERADOR. 11. CONCLUSIONES

1. INTRODUCCIÓN

En este estudio ofrecemos algunas ideas sobre los rasgos básicos del seguro de responsabilidad civil profesional de los operadores de inteligencia artificial¹ a la vista del Reglamento de Inteligencia Artificial Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (RIA)².

Realizamos el diseño básico del seguro de responsabilidad civil profesional de los operadores de inteligencia artificial sobre la base de la normativa común porque los intentos de armonizar un régimen de la responsabilidad civil derivada del uso de la inteligencia artificial y unificar la exigencia de un seguro de responsabilidad civil obligatorio para los sistemas de inteligencia artificial de alto riesgo no han visto la luz, según se deduce de lo relatado en el epígrafe siguiente, dedicado a los antecedentes.

¹ El lector interesado en la materia puede consultar nuestros estudios sobre “La Responsabilidad Civil derivada del uso de la Inteligencia Artificial y su Aseguramiento” publicado en la Revista Ibero-Latinoamericana de Seguros, Vol. 30, Núm. 54, 2021, pp. 107-146; “La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento” publicado en la Revista de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro n.º 76 (2020), pp. 79 a 104; “Decálogo de la inteligencia artificial ética y responsable en la Unión Europea”, publicado en La Ley Unión Europea n.º 87, Sección Doctrina y en el Diario La Ley, 30 de diciembre de 2020; “Digitalización financiera en la Unión Europea novedades regulatorias ciberresiliencia operativa, inteligencia artificial y cryptoactivos”, publicado en La Ley Unión Europea, n.º 97, Sección Regulación, noviembre 2021 y en Diario La Ley de 30 de noviembre de 2021. También puede consultar la entrada de nuestro blog de 17.05.2022 dedicada al “Congreso Internacional sobre “La inteligencia artificial en el Derecho de daños” organizado por el Departamento de Derecho Civil de la Universidad de Alicante los próximos días 23 y 24 de mayo de 2022. El seguro y la inteligencia artificial”. Por último, recomendamos vivamente la lectura del número 100 correspondiente a los meses de septiembre y octubre de 2022 sobre “inteligencia Artificial y Derecho” de la revista El Cronista del Estado Social y Democrático de Derecho y, en particular, su prólogo, pp. 5 a 13, a cargo del Profesor Santiago Muñoz Machado).

² El lector interesado puede ver las 5 entradas de nuestro blog financiero (ajtapia.com) dedicadas a los aspectos generales, la estructura y el funcionamiento de este RIA publicadas los días 22, 24, 26, 29 y 30 de julio de 2024.

2. ANTECEDENTES

2.1. LA RESOLUCIÓN DEL PARLAMENTO EUROPEO SOBRE UN RÉGIMEN DE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL DE 20 DE OCTUBRE DE 2020

La Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) (RIAR) que lleva por título “Régimen de responsabilidad civil en materia de inteligencia artificial”³ incluía, en su Anexo, una Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial en la que se decía que su objeto consistiría en “establecer normas en relación con las demandas por responsabilidad civil de las personas físicas y jurídicas contra los operadores de sistemas de IA” (art.1) y su ámbito de aplicación se extendería, “en el territorio de la Unión a aquellos casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable” (art.2).

Una vez fijado su objetivo y su ámbito de aplicación, la Propuesta de Reglamento aneja a la RIAR distinguía dos regímenes de responsabilidad civil derivada de los sistemas de IA de acuerdo con su grado de riesgo respectivo. En primer lugar, un régimen de responsabilidad objetiva de los sistemas de IA de alto riesgo que se establecía diciendo que “el operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA”. Adviértase que la Propuesta preveía que el anexo al Reglamento enumeraría todos los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan y la Comisión estaría facultada para adoptar actos delegados para modificar dicha lista exhaustiva (art.4). En segundo lugar, un régimen de responsabilidad por culpa para el resto de sistemas de IA.

Como un elemento típico de las regulaciones de los sistemas de responsabilidad civil objetiva se establecía su cobertura preventiva mediante la exigen-

³ P9_TA-PROV(2020)0276. Se puede consultar la entrada de nuestro blog financiero (ajtapia.com) de 13 de noviembre de 2020 sobre “Digitalización financiera: Los 3 principios regulatorios de una Inteligencia Artificial Responsable (IAR) en la UE. Resolución del Parlamento Europeo de 20 de octubre de 2020 sobre la responsabilidad civil en materia de inteligencia artificial”.

cia de un seguro obligatorio de responsabilidad civil para los operadores de sistemas de IA de alto riesgo. El diseño inicial de este seguro se basaba en el régimen del seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles⁴. De tal modo que el Parlamento Europeo -en el apartado 24 de la RIAR- consideraba que debía establecerse un régimen de seguro obligatorio para los sistemas de IA de alto riesgo que debía cubrir los importes y el alcance de la indemnización establecidos por el Reglamento propuesto a la Comisión Europea que figuraba como Anexo a la RIAR. Y, para el diseño de ese seguro,. De modo tal que todos los operadores de sistemas de IA de alto riesgo deberían ser titulares de un seguro de responsabilidad civil.

Una vez establecida esta necesidad de un seguro obligatorio para los sistemas de IA de alto riesgo análogo al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles; la RIAR apuntaba las dificultades que su implantación conllevaría que pueden exponerse en forma de causa y efecto: a) La causa era la falta de estadísticas de siniestralidad, porque esta ausencia de datos sobre los riesgos asociados a los sistemas de IA, unida a la incertidumbre sobre su evolución en el futuro, dificultaba al sector de los seguros elaborar productos de seguro nuevos o adaptados. b) El efecto consistía en el riesgo de que el mercado asegurador diseñara un seguro obligatorio de “talla única” con primas desproporcionadamente elevadas y los incentivos equivocados, alentando a los operadores a optar por el seguro más barato en lugar de por la mejor cobertura, lo que podría convertirse en un obstáculo para la investigación y la innovación. De ahí infería “que la Comisión debe colaborar estrechamente con el sector de los seguros para estudiar la forma de poder utilizar datos y modelos innovadores para crear pólizas de seguro que ofrezcan una cobertura adecuada a un precio asequible”.

⁴ En concreto, tomaba como modelo la Directiva 2009/103/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad. En este sentido, el PE opinaba que “sobre la base del potencial significativo para causar un daño o un perjuicio y teniendo en cuenta la Directiva 2009/103/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad, todos los operadores de sistemas de IA de alto riesgo enumerados en el anexo del Reglamento propuesto deben ser titulares de un seguro de responsabilidad civil; considera que ese régimen de seguro obligatorio para los sistemas de IA de alto riesgo debe cubrir los importes y el alcance de la indemnización establecidos por el Reglamento propuesto; es consciente de que actualmente dicha tecnología es todavía muy inusual, ya que presupone un alto grado de toma de decisiones autónomas, y de que, por consiguiente, los debates actuales están orientados sobre todo al futuro; cree, no obstante, que la incertidumbre relacionada con los riesgos no debe hacer que las primas de seguro sean prohibitivamente elevadas y convertirse así en un obstáculo para la investigación y la innovación” (apartado 24 de la RIAR).

Por último, PE advertía “que un mecanismo de indemnización a escala de la Unión, financiado con fondos públicos, no es la manera adecuada de colmar posibles lagunas en materia de seguros”. (apartado 25 de la RIAR).

2.2. LA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD EN MATERIA DE INTELIGENCIA ARTIFICIAL DE 28 DE SEPTIEMBRE DE 2022

El día 28 de septiembre de 2022, la Comisión Europea publicó la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA) (PDRIA)⁵.

El objetivo de la DRIA consistirá en establecer requisitos uniformes para determinados aspectos de la responsabilidad civil extracontractual por los daños causados con mediación de sistemas de IA. En este sentido, daba continuidad a la Resolución del Parlamento Europeo 2020/2014 (INL)⁶.

Dado que la DRIA parte de la base del respeto a los sistemas nacionales de responsabilidad civil que presentan variaciones entre los Estados miembros de la UE; su alcance resulta eminentemente procesal y, más en concreto, en materia de prueba. Como así consta desde su art.1.1 que comienza diciendo: “La presente Directiva establece normas comunes sobre: a) la exhibición de pruebas relativas a sistemas de inteligencia artificial (IA) de alto riesgo con el fin de permitir a los demandantes fundamentar sus demandas de responsabilidad civil extracontractual subjetiva (basada en la culpa) por daños y perjuicios; b) la carga de la prueba en el caso de demandas de responsabilidad civil extracontractual subjetiva (basada en la culpa) interpuestas ante tribunales nacionales por daños y perjuicios causados por sistemas de IA”. En este sentido, las herramientas de “probática” que utiliza la DRIA y, especialmente, las presunciones de causalidad eficiente que veremos no son nuevas; sino que pueden encontrarse en los sistemas legislativos nacionales (por ejemplo, en nuestro Código Civil y en nuestra LEC). Por lo tanto, estas herramientas nacionales constituyen puntos de referencia útiles sobre cómo abordar las cuestiones planteadas por la IA en relación con las normas de responsabilidad en

⁵ Bruselas, 28.9.2022, COM(2022) 496 final, 2022/0303 (COD), Texto pertinente a efectos delEEE, SEC(2022) 344 final} - {SWD(2022) 318 final} - {SWD(2022) 319 final} -{SWD(2022) 320 final}. El lector puede consultar las dos entradas de nuestro blog de 14 y 15 de diciembre de 2022 sobre “Inteligencia Artificial Responsable (IAR): la Propuesta de Directiva sobre responsabilidad en materia de IA de 28 de septiembre de 2022”.

⁶ De la que dimos noticia en la entrada de nuestro blog de 17.10.2021 sobre las “Finanzas digitales (Fintech): Inteligencia artificial, responsabilidad civil y seguro: La Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre el “Régimen de responsabilidad civil en materia de inteligencia artificial”,

vigor de manera que se interfiera lo menos posible en los diferentes regímenes jurídicos nacionales.

3. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

En el DOUE del viernes, 12 de julio, se publicó el Reglamento de Inteligencia Artificial⁷ que marca el contexto normativo en el que se debe diseñar el seguro de responsabilidad civil profesional de los operadores de sistemas de IA. En concreto y con referencia a estos últimos, tipifica una serie de operadores de sistemas de IA que serán los tomadores y asegurados del seguro de responsabilidad civil profesional cuyas líneas básicas exponemos en este Estudio. En particular, el operador es la categoría general (art.3.8) que abarca a:

- a) Los proveedores, definidos como “una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente” (art.3.3). Dentro de esta categoría podemos incluir a los proveedores posteriores, y a sus representantes autorizados.
- b) Los fabricantes del producto.
- c) Los responsables del despliegue definidos como “una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se

⁷ Para la comprensión de este RIA -denominado Ley Europea de Inteligencia Artificial (LEIA)- resulta particularmente útil el Documento de preguntas y respuestas que publicó la Comisión Europea el 1 de agosto de 2024. Ref. QANDA/21/1683. Inteligencia artificial Preguntas y respuestas Actualizado el 01/08/2024. Brussels, 1 de agosto de 2024). A este Documento nos referimos en las entradas de nuestro blog financiero publicadas los días 12, 13 y 14 de agosto de 2024 con el título común de “Ley Europea de Inteligencia Artificial (LEIA): Preguntas y respuestas. Documento de la Comisión Europea de 1 de agosto de 2024”. Este Documento de preguntas y respuestas destaca los aspectos críticos de la LEIA como, por ejemplo, las diferentes categorías de riesgos, la transparencia exigible a los sistemas de IA generativa, la identificación biométrica, la compatibilidad con los derechos fundamentales y la propiedad intelectual, el sistema de gobernanza de la LEIA, Código de buenas prácticas para los proveedores de modelos de IA de uso general, etc. En todos estos ámbitos, el documento de la Comisión nos ofrece información especialmente valiosa que complementa el contenido de la LEIA con ejemplos (por ejemplo, de sistemas de IA de alto riesgo), con datos técnicos (por ejemplo, de modelos de IA de uso general que general riesgos sistémicos porque hayan sido entrenados utilizando una potencia informática total de más de 10 a 25 FLOP) y con explicaciones de aspectos de la gestión de la LEIA (por ejemplo, los encargos de la Comisión Europea a las organizaciones europeas de normalización CEN y CENELEC para la elaboración de normas para los requisitos exigibles a los sistemas de IA de alto riesgo).

enmarque en una actividad personal de carácter no profesional” (art.3.4).

- e) Los importadores, definidos como “una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país” (art.3.6).
- f) Los distribuidores, definidos como “una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión” (art.3.7).

4. LAS CARACTERÍSTICAS DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

4.1. SEGURO VOLUNTARIO

Según vimos en el epígrafe II de este Estudio, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial que obraba como Anexo a la Resolución del Parlamento Europeo de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) señalaba que todos los operadores de sistemas de IA de alto riesgo debían ser titulares de un seguro de responsabilidad civil. Este carácter obligatorio tendría, en nuestro Ordenamiento consecuencias regulatorias particularmente relevantes⁸.

Sin embargo, finalmente el RIA no establece -entre las obligaciones de los operadores en la gestión de los sistemas de IA de alto riesgo (art.16)- la obligación de contratar un seguro de responsabilidad civil profesional. En particular, aquel seguro no se incluye en el sistema de gestión de la calidad que deben es-

⁸ Resultan de especial interés las consideraciones que hacía Fernando Sánchez Calero al comentar el anteriormente vigente art.75 de la LCS en Sánchez Calero F., *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre y a sus modificaciones*, 4ª ed. (2010), Thomson Reuters, p. 1700 y ss. Sobre los efectos de esta obligatoriedad prevista en la Disposición adicional segunda de la LOSSEAR sobre en unos seguros de responsabilidad civil profesional pueden verse nuestro estudio sobre “Los seguros obligatorios de responsabilidad civil de los mediadores y de los administradores concursales”. Cuadernos de Derecho y Comercio. Derecho concursal: cuestiones actuales, Extraordinario 2016, Consejo General del Notariado, pp. 643-665. Ver nuestra Guía del Contrato de Seguro, 2ª ed., Colección Monografías Aranzadi, Aranzadi, Cizur Menor (2022), p. 273 y ss.

tablecer los proveedores de sistemas de IA de alto riesgo (art.17)⁹ ni de sistemas de IA de uso general de riesgo normal (art.53) o de los que impliquen un riesgo sistémico (art.55). Por lo tanto, estaremos ante un seguro voluntario.

4.2. SEGURO DE RESPONSABILIDAD CIVIL EMPRESARIAL O PROFESIONAL

Esta característica circunscribe la cobertura del seguro a las responsabilidades civiles en las que pueda incurrir el operador de inteligencia artificial en su condición de tal, con un doble alcance empresarial y profesional. Sin perjuicio de esta delimitación empresarial o profesional, una vez llegados a este ámbito, se debe prestar una cobertura omnicomprendensiva, tanto en sentido subjetivo, al cubrir al operador y, en su caso, sus empleados¹⁰; como en sentido objetivo, al abarcar las responsabilidades derivadas de los usos de la inteligencia artificial tanto directos como conexos. En términos generales, hay que resaltar la importancia que tiene, dentro de la jurisprudencia sobre seguros de responsabilidad civil, la delimitación precisa de la actividad asegurada en la póliza.

5. LAS PARTES

5.1. EL ASEGURADOR

Deberá ser una entidad aseguradora autorizada para desarrollar el ramo de “responsabilidad civil en general”¹¹.

En la práctica, tanto la importancia cuantitativa y cualitativa de la cobertura necesaria como el principio de reparto de cuotas de dicha cobertura podría hacer recomendable, en determinados casos, adoptar la estructura de coaseguro que se caracteriza por la coincidencia de las coberturas de los diferentes coaseguradores, con reparto de cuotas y responsabilidad proporcional, sin

⁹ El Documento de preguntas y respuestas que publicó la Comisión Europea el 1 de agosto de 2024 se refiere a estas obligaciones cuando responde a la pregunta: “¿Cuáles son las obligaciones de los proveedores de sistemas de IA de alto riesgo?”.

¹⁰ En este sentido, es interesante recordar que el artículo 4 del RIA -dedicado a La “Alfabetización en materia de IA”- dispone que “los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas”.

¹¹ Ramo 13 de los Ramos de seguro distintos del seguro de vida enumerados en el Anexo de la LOSSEAR.

solidaridad y con encomienda a la entidad aseguradora abridora de gestión común con interlocución única frente al tomador y asegurados. Todo ello conforme a lo dispuesto en el art.33 de la LCS.

5.2. EL TOMADOR Y EL ASEGURADO. LAS PÓLIZAS COLECTIVAS

Actuará como tomador el operador profesional del sistema de inteligencia artificial (nos remitimos a la tipificación que de ellos hace el RIA a la que nos referimos en el epígrafe III de este Estudio) que generalmente, actuará también como asegurado por cuenta propia; sin perjuicio de la posibilidad de contratar seguros colectivos por asociaciones de operadores de IA, grupos de empresas u otras personas jurídicas con forma de sociedad mercantil de capital que actúen como operadores profesionales de sistemas de inteligencia artificial. Se trata de una posibilidad extremadamente interesante en la práctica ya que produciría, previsiblemente, un importante ahorro de costes a la asociación o entidad tomadora en forma de abaratamiento de primas respecto de la contratación individual (v. art.7 LCS).

Según decimos, el operador profesional del sistema de inteligencia artificial, como potencial responsable civil, será el titular del interés asegurado. Reiteramos el interés que acabamos de indicar que tendrán los seguros colectivos en este ámbito, en los que una asociación de empresas de IA o la matriz de un grupo de sociedades dedicadas a operar en sistemas de IA, especialmente si son de alto riesgo; podrán contratar -como tomadoras- seguros colectivos que cubran la responsabilidad civil de las empresas de IA asociadas o filiales. Fórmula que ofrecerá dos ventajas evidentes: la primera es la mejor racionalización de la gestión de la cobertura de los riesgos derivados de la IA a nivel de grupo y la segunda ventaja es el presumible ahorro de costes por disminución del importe de las primas de estas pólizas colectivas frente al sumatorio de tantas pólizas individuales como operadores asegurados.

6. EL RÉGIMEN DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

6.1. SEGURO DE RÉGIMEN COMÚN O SEGURO POR GRANDES RIESGOS

El seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial se calificará como un seguro por grandes riesgos

cuando reúna los criterios establecidos en el art. 11 de la LOSSEAR. En tal caso, se le aplicará la previsión del art. 44 de la LCS, por lo que los preceptos de esta LCS se le aplicarán con carácter dispositivo.

Cuando el seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial no reúna los criterios establecidos en el art. 11 de la LOSSEAR, se calificará como un seguro de régimen común al que los preceptos de la LCS se le aplicarán con carácter imperativo conforme al art. 2 de esa misma LCS. Procede destacar que esta imperatividad busca la protección tanto del operador de IA asegurado como del tercero perjudicado titular de la acción directa que le otorga el ar.76 de la LCS).

6.2. APLICACIÓN DE LA LCS

Al seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial procederá aplicarle la LCS conforme a la siguiente sucesión lógica de preceptos: los que regulan el seguro de responsabilidad civil (sección 8ª del título II, arts. 73 a 76)¹², las disposiciones generales de los seguros de daños (sección 1ª del título II, arts. 25 a 44) y las disposiciones generales sobre los contratos de seguro (título I, arts. 1 a 24).

6.3. APLICACIÓN DE LA LOSSEAR

Además de la normativa contractual antedicha, el asegurador en el seguro examinado estará sujeto a los deberes que le impone la normativa de ordenación y supervisión a través de la LOSSEAR y el ROSSEAR. En cuanto se refiere al contrato de seguro, estos deberes se establecen, fundamentalmente, en las “conductas de mercado” que deben seguir los aseguradores (capítulo VII del título III) y, más en concreto, en los deberes de información al tomador del seguro y a los asegurados que se corresponden con otros tantos derechos de estos últimos (art. 96 LOSSEAR y art. 122 ROSSEAR).

¹² Ver, por todos, los comentarios de Fernando Sánchez Calero a estos preceptos en Sánchez Calero F., *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre y a sus modificaciones*, cit. p. 1589 y ss. Ver también nuestra *Guía del Contrato de Seguro* cit., p. 226 y ss.

7. LA DELIMITACIÓN SUSTANCIAL DEL RIESGO CUBIERTO POR REFERENCIA A LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

7.1. DEFINICIÓN GENERAL DEL RIESGO CUBIERTO

El seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial¹³ será un contrato de seguro por el que el asegurador se obliga, dentro de los límites establecidos en la Ley y en la póliza, a cubrir el riesgo del nacimiento a cargo de los operadores de sistemas de inteligencia artificial de la obligación de indemnizar a una persona física o jurídica usuaria de tales sistemas por los daños y perjuicios causados por una actuación del propio operador o del personal empleado prevista en el contrato de cuyas consecuencias sea civilmente responsable.

En este sentido, resultará esencial para la valoración del riesgo cubierto la clasificación del RIA de los sistemas de IA de alto riesgo, por estar integrados en determinados productos o por impactar en determinados ámbitos; los sistemas de IA de uso de riesgo normal o que impliquen un riesgo sistémico porque cada tipo de sistema de IA implicará diferentes obligaciones de sus operadores, cuyo incumplimiento podrá ser la causa del daño causado del que será civilmente responsable el operador.

En la práctica, las pólizas definirán como actividad asegurada el desarrollo de los diferentes sistemas de inteligencia artificial en el ejercicio de la actividad profesional del operador, incluyendo las actuaciones y gestiones previas, posteriores y complementarias al ejercicio de aquella actividad.

7.2. DESCRIPCIÓN ESPECÍFICA DE LOS RIESGOS EXCLUIDOS DE LA COBERTURA

En la práctica, las pólizas excluirán la responsabilidad civil derivada de una actuación dolosa del operador o del desarrollo de actividades ajenas al ejercicio de su actividad profesional de desarrollo de sistemas de inteligencia artificial, así como los daños causados al propio operador por infidelidades de sus empleados.

¹³ En este punto, conviene recordar la definición de «sistema de IA» del art.3.1 del RIA como “un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales”.

En todo caso, hay que tener en cuenta que la exclusión de cobertura en caso de actuación dolosa del operador no excluirá su defensa jurídica frente a reclamaciones, si bien concede al asegurador un derecho de repetición frente al operador en caso de acreditación de su actuación dolosa.

8. LA DELIMITACIÓN TEMPORAL DEL RIESGO CUBIERTO POR REFERENCIA A LAS RECLAMACIONES PRESENTADAS CONTRA EL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO. LAS CLÁUSULAS “CLAIMS MADE”

El análisis de las características previsibles de las futuras reclamaciones de la responsabilidad civil a los operadores de los sistemas de inteligencia artificial en sus diferentes niveles de riesgo; nos permite vaticinar que sus negligencias profesionales se podrán manifestar pasado un tiempo desde el momento de su comisión. Es por ello por lo que, en este tipo de seguros de responsabilidad civil profesional, tiene particular importancia la delimitación temporal del riesgo cubierto. Ello es así porque, con frecuencia, el daño en el patrimonio del usuario de un sistema de inteligencia artificial se manifestará pasado un tiempo desde la intervención del operador y, por ello, la reclamación del tercero perjudicado o de sus herederos se formulará en ese momento. En tal caso, es posible que, durante ese periodo de tiempo, haya sobrevenido un periodo de seguro distinto. Lo cual no planteará problemas de cobertura si continúa actuando el mismo asegurador en ambos periodos; pero si puede plantearlos si hay un cambio el asegurador.

Lo anterior nos lleva a recordar que, en este tipo de seguro, existen dos acontecimientos fundamentales para determinar la cobertura del asegurador que son, por su orden cronológico: primero, el hecho causante o generador del daño, que consistirá en la utilización del sistema de inteligencia artificial, acaecido en el día X; y, segundo, la reclamación del usuario de aquel sistema que resulte perjudicado que será posterior a la manifestación del daño o lesión patrimonial, acaecida en el día Y, siendo Y posterior a X. Cabría referirse, basándose en la doctrina jurisprudencial, a tres hechos relevantes: la utilización del sistema de inteligencia artificial; el de la ocurrencia o manifestación del daño y el de la formulación de la reclamación contra el operador por parte del usuario perjudicado.

Es importante señalar que la jurisprudencia de la Sala Primera de lo Civil del Tribunal Supremo tiene reiteradamente establecido –sobre la base del párrafo primero del art. 73 de la LCS que, como antes vimos, se refiere al “nacimiento a cargo del asegurado de la obligación de indemnizar a un tercero

los daños y perjuicios causados por un hecho previsto en el contrato”- que el momento decisivo para determinar la cobertura del asegurador es aquel en el que se produce el hecho generador de la responsabilidad civil. Que, en este seguro será el acto o intervención del operador del sistema de inteligencia artificial.

Lo anterior significa que la póliza de seguro de responsabilidad civil profesional del operador de los sistemas de inteligencia artificial deberá cubrir a los operadores asegurados frente a reclamaciones que deriven de actos o intervenciones acaecidas en el periodo de seguro, con independencia del momento en el que aquellas reclamaciones se formulen; si bien puede limitar aquellas reclamaciones siempre que se cumplan la garantías establecidas en el segundo párrafo del art. 73 de la LCS, a las que nos referimos seguidamente. En efecto, partiendo de la distinción anterior, entre el hecho causante (utilización del sistema de inteligencia artificial) y la reclamación del usuario como tercero perjudicado o de sus herederos, podemos distinguir dos hipótesis temporales: a) La primera es cuando la utilización del sistema de inteligencia artificial (hecho causante) y la reclamación del usuario perjudicado coinciden en el período de vigencia de la póliza. En este caso de coincidencia temporal no hay duda razonable sobre la cobertura por parte del asegurador de la responsabilidad civil reclamada de ese periodo. b) La segunda se produce cuando solo uno de tales hechos acaece en el período de seguro. A su vez, pueden darse dos situaciones de divergencia temporal: La primera se producirá cuando la utilización del sistema de inteligencia artificial anterior al período de seguro da origen a una reclamación durante la vigencia de la póliza. La segunda se produce cuando la utilización del sistema de inteligencia artificial acaecida durante la vigencia de la póliza da lugar a una reclamación posterior.

Para permitir la programación en las pólizas de ambas hipótesis y por razones de seguridad jurídica, el legislador introdujo un segundo párrafo en el art. 73 de la LCS para fijar las condiciones de admisibilidad de las cláusulas que delimitan la cobertura de los seguros de responsabilidad civil por referencia a las reclamaciones (las denominadas “claims made”).

Por lo tanto, resulta admisible excluir la cobertura del asegurador mediante la correspondiente cláusula limitativa en la póliza de seguro que deje fuera las reclamaciones realizadas más allá del año siguiente al término del período de seguro o los usos del sistema de inteligencia artificial acaecidos con una antelación superior a un año al inicio de efectos de la póliza. Y, por esta misma razón, a falta de cláusulas limitativas en los sentidos indicados, el asegurador responderá de la cobertura de la responsabilidad civil del operador asegurado derivada de la utilización del sistema de inteligencia artificial acaecida durante el período de vigencia de la póliza, con independencia del

momento en que se produzca la reclamación del usuario perjudicado, siempre que el tercer perjudicado demuestre que el hecho causante se produjo en el período del seguro y ello porque la Jurisprudencia da primacía al propio hecho causante.

En la práctica, las pólizas delimitarán temporalmente el riesgo cubierto por referencia a la presentación formal de la reclamación frente al operador del sistema de inteligencia artificial (mediante comunicación escrita, carta, fax, telegrama, etc.) durante el periodo de vigencia de la póliza, con independencia de que el hecho causante se haya producido antes de la vigencia de la póliza (siempre que fuera desconocido) o durante dicha vigencia.

9. LA DEFENSA JURÍDICA DEL OPERADOR DE SISTEMAS DE INTELIGENCIA ARTIFICIAL ASEGURADO FRENTE A LA RECLAMACIÓN DEL USUARIO PERJUDICADO O DE SUS HEREDEROS

En estos seguros de responsabilidad civil de los operadores de sistemas de inteligencia artificial, por regla general y en un principio, el asegurador asumirá la dirección jurídica frente a la reclamación del usuario perjudicado contra el operador y serán de su cuenta los gastos de defensa que se ocasionen. Y el operador asegurado deberá prestar la colaboración necesaria en orden a la dirección jurídica asumida por el asegurador (art.74 LCS)¹⁴.

La regla general anterior cuenta con dos excepciones, todo ello conforme a lo dispuesto en el art.74 de la LCS: a) La primera es voluntaria u optativa y consiste en que la póliza otorgue al operador tomador y asegurado la facultad de elegir al abogado o procurador que asuma la dirección jurídica de su defensa, cubriendo el asegurador los gastos consiguientes. En la práctica, cuando un seguro de responsabilidad civil profesional reconoce al asegurado dicha facultad (lo que sucede, por ejemplo, en algunos seguros de responsabilidad civil de administradores y directivos de sociedades, denominados seguros de D&O), el asegurador se reserva la aprobación previa de los honorarios del abogado elegido o admite “ab initio” los honorarios de los abogados de un “panel” de firmas legales relacionadas en un anexo de la póliza. b) La segunda excepción es obligatoria y nace cuando quien reclame

¹⁴ Ver, por todos, el comentario del art.74 de la LCS por Fernando Sánchez Calero en Sánchez Calero F., Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre y a sus modificaciones, cit. p. 1589 y ss. Ver también nuestra Guía del Contrato de Seguro cit., p. 266 y ss.

esté también asegurado con el mismo asegurador o exista algún otro posible conflicto de intereses porque, en este caso, el asegurador deberá comunicar de inmediato al operador de sistemas de inteligencia artificial asegurado y demandado la existencia de esas circunstancias para que asegurado pueda optar entre mantener la dirección jurídica por el asegurador o confiar su propia defensa a otra persona, abonando el asegurador los gastos de tal dirección jurídica hasta el límite pactado en la póliza. Y todo ello sin perjuicio de que el asegurador deberá realizar aquellas diligencias que por su carácter urgente sean necesarias para la defensa del al personal de enfermería asegurado y demandado.

10. LA ACCIÓN DIRECTA DEL USUARIO DE UN SISTEMA DE INTELIGENCIA ARTIFICIAL PERJUDICADO O SUS HEREDEROS CONTRA EL ASEGURADOR DEL OPERADOR

Al amparo del seguro de responsabilidad civil de los operadores de sistemas de inteligencia artificial, el usuario perjudicado por la actuación profesional dañosa del operador asegurado o sus herederos podrán dirigir una acción directa contra el asegurador para exigirle el cumplimiento de la obligación de indemnizar. Frente a esta acción directa, el asegurador no podrá oponer al tercero perjudicado las excepciones que tenga frente al notario asegurado; pero si podrá oponer la culpa exclusiva del perjudicado y las excepciones personales que tenga contra éste (art.76 LCS)¹⁵.

En relación con lo anterior, hay que hacer dos precisiones que afectan a otras tantas relaciones: a) Primera, a la relación entre el operador de sistemas de inteligencia artificial asegurado y el asegurador porque, si el siniestro ha sido fruto de una conducta dolosa del operador asegurado, el asegurador, después de pagar la indemnización al tercero perjudicado o a sus herederos, tendrá derecho de repetición contra el operador asegurado. b) Segunda, a la relación entre el operador de sistemas de inteligencia artificial y el usuario perjudicado, porque el primero está obligado a manifestar al tercero perjudicado o a sus herederos la existencia del contrato de seguro y su contenido. Todo ello conforme a lo dispuesto en el art. 76 de la LCS.

¹⁵ Ver, por todos, el comentario del art.76 de la LCS por Fernando Sánchez Calero en Sánchez Calero F., Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre y a sus modificaciones, cit. p. 1721 y ss. Ver también nuestra Guía del Contrato de Seguro cit., p. 250 y ss.

11. LA TRANSPARENCIA DE LAS CONDICIONES DEL SEGURO DE RESPONSABILIDAD CIVIL DE LOS OPERADORES DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Según adelantamos al hablar de la aplicación a este seguro de las normas de ordenación y supervisión contenidas en la LOSSEAR y en el ROSSEAR, el impacto fundamental de esta normativa de ordenación se produce en cuanto a los deberes de información al tomador del seguro y al operador asegurado¹⁶. En concreto, estos deberes de los aseguradores - que se corresponden con otros tantos derechos de los primeros- inciden en los tres aspectos siguientes: En la información previa general que debe ofrecer el asegurador sobre su identificación y el régimen de las eventuales reclamaciones. En la información previa específica que debe ofrecer en los seguros colectivos a través de los boletines de adhesión o certificados de seguro. En la información financiera y de solvencia del asegurador.

12. CONCLUSIONES

Primera. El aseguramiento de la responsabilidad civil de los operadores de sistemas de inteligencia artificial se realizará mediante un seguro de responsabilidad civil que presentará tres características esenciales: seguro voluntario y seguro de responsabilidad civil empresarial o profesional que podrá estructurarse como un seguro individual o colectivo.

Segunda. El seguro de responsabilidad civil de los de los operadores de sistemas de inteligencia artificial deberá basar su régimen en la normativa sustancial específica del RIA y, a partir de ella, se regirá por la Ley de Contrato de Seguro, que se aplicará con carácter imperativo por regla general o dispositivo si se trata de un seguro por grandes riesgos que cumpla los requisitos del art.11 de la LOSSEAR. Todo ello sin perjuicio de que el asegurador deba cumplir con las normas de conducta –especialmente en materia de documentación e información-que le imponen la LOSSEAR y el ROSSEAR.

Tercera. Los puntos críticos del seguro de responsabilidad civil de los operadores de sistemas de inteligencia artificial serán: la delimitación material de la cobertura, con las inclusiones y exclusiones pactadas en la póliza; la delimitación temporal de la cobertura, con la precisión de las reclamaciones cubiertas; el régimen de la defensa jurídica del operador demandado y de la acción directa del usuario perjudicado frente a la aseguradora.

¹⁶ V el art. 96 de la LOSSEAR y el art. 122 del ROSSEAR.

Cuarta. Es más que previsible que las reclamaciones de responsabilidad civil contra los operadores de sistemas de inteligencia artificial se multipliquen tanto en su número como en su cuantía en un futuro próximo tanto por razones generales, como es la extensión de la denominada “cultura de la reclamación” que rige en las sociedades desarrolladas respecto de las actividades económicas y las profesiones en general; como por razones específicas, como son la digitalización creciente de la economía y, en particular, la extensión imparable de los sistemas de IA en todo tipo de actividades.

Quinta. El diseño adecuado del seguro de responsabilidad civil de los operadores de sistemas de inteligencia artificial deberá producir un doble y recíproco beneficio: para los operadores, cuyo patrimonio se mantendrá indemne frente a las reclamaciones de los usuarios perjudicados; y para los usuarios, que contarán con la garantía preventiva y adicional prestada por el asegurador.

GRACIAS POR CONFIAR EN NUESTRAS PUBLICACIONES

Al comprar este libro le damos la posibilidad de consultar gratuitamente la versión ebook.

Cómo acceder al ebook:

- ☞ **Entre en nuestra página web**, sección Acceso ebook
(www.dykinson.com/acceso_ebook)
- ☞ **Rellene el formulario** que encontrará insertando el código de acceso que le facilitamos a continuación así como los datos con los que quiere consultar el libro en el futuro (correo electrónico y contraseña de acceso).
- ☞ Si ya es **cliente registrado**, deberá introducir su **correo electrónico y contraseña habitual**.
- ☞ Una vez registrado, **acceda a la sección Mis e-books de su cuenta de cliente**, donde encontrará la versión electrónica de esta obra ya desbloqueada para su uso.
- ☞ Para consultar el libro en el futuro, ya sólo es necesario que se identifique en nuestra web con su correo electrónico y su contraseña, y que se dirija a la sección Mis ebooks de su cuenta de cliente.



CÓDIGO DE ACCESO

Rasque para ver el código

Nota importante: Sólo está permitido el uso individual y privado de este código de acceso. Está prohibida la puesta a disposición de esta obra a una comunidad de usuarios.



**MANTÉNGASE INFORMADO
DE LAS NUEVAS PUBLICACIONES**

**Suscríbase gratis
al boletín informativo
www.dykinson.com**

Y benefíciase de nuestras ofertas semanales

La inteligencia artificial tiene el potencial de transformar productos, servicios y procedimientos en multitud de sectores económicos y en relación con muchos ámbitos de la sociedad. Sin embargo, también puede generar un sinnúmero de riesgos que, de producir daños, habrán de ser reparados. La Unión Europea no ha sido ajena a estos riesgos, y por ello ha pretendido y sigue pretendiendo crear un marco jurídico protector. Dentro de este contexto, se sitúa la aprobación del Reglamento (UE) 1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial -RIA-, como sendas Propuestas de Directiva, de inminente aprobación, sobre responsabilidad civil de productos defectuosos y sobre responsabilidad civil por daños causados por la inteligencia artificial. Partiendo de tales postulados, en la presente obra se han seleccionado aquellos sectores donde, por su mayor proyección, novedad o complejidad, merece ser analizada la interrelación entre la tecnología de la inteligencia artificial y el Derecho de daños. Para ello, se ha podido contar con un elenco de especialistas en el sector, que sin duda hace de la obra resultante una aportación doctrinal de indudable utilidad.

Con carácter particular, entre los sectores seleccionados, destaca por su trascendencia, el de la salud digital, donde problemáticas relacionadas con sistemas inteligentes para la prevención de enfermedades, ya sea a iniciativa del profesional de la medicina, o al margen de él -uso de wearables y servicios digitales-, o por infracciones de los datos personales de salud, pueden determinar, si bien a través de distintos cauces normativos, posibles vías de reclamación indemnizatoria.

En el campo quirúrgico, la “cirugía 4.0”, que integra la cirugía robótica y personalizada, por su creciente implantación, ha merecido una especial consideración en la obra.

Se efectúan igualmente amplias consideraciones acerca de la transparencia y explicabilidad para prevenir la discriminación algorítmica en el uso de los sistemas de inteligencia artificial.

Dentro de los sectores con mayor implementación de las tecnologías de inteligencia ha sido objeto de consideración así mismo el uso de vehículos autónomos, incluida su problemática en la vertiente del Derecho internacional privado.

Situados en el marco normativo que proporciona el Reglamento de Inteligencia artificial -RIA- se efectúan correspondientes análisis acerca de la categorización del riesgo que el mismo contempla, y donde se observa un régimen jurídico tendente a salvaguardar los riesgos más graves por el empleo de los sistemas de inteligencia artificial; en particular, en la salud, seguridad y derechos consagrados en la Carta Europea de Derechos Fundamentales. De igual forma las implicaciones jurídicas que despliega la inteligencia artificial generativa por infracciones normativas del Derecho de protección de datos personales. Se incluyen también los rasgos que deben estar presentes en el seguro de responsabilidad civil profesional de los operadores de inteligencia artificial, a partir de las previsiones normativas del referido Reglamento de Inteligencia Artificial.

