



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

Dykinson, S.L.

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

**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	

Dykinson, S.L.

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 REGÍMENES 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 DEEPFAKE Y SU CLASIFICACIÓN DEL RIESGO.....	225
3. PROBLEMÁTICA JURÍDICA DEL DEEPFAKE.....	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 *werables* 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>WERABLES</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. <i>Soft law</i> público y avances legislativos	331
3. PROTECCIÓN DISPENSADA A LOS NEURODATOS POR EL RE- GLAMENTO (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 dere- cho 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 BALMASEDA

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

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 I, 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 eliminen 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 «robot¹⁸».

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 robotizados 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-

paran, 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 (subjettiva) 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 biomechanics: artificial intelligence and time-frequency analysis. En *Applied Biomechanics 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.

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.

