DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

7

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

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
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.

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-100) 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.

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

Perspectiva y categorización del riesgo en el Reglamento de Inteligencia Artificial

Miquel Peguera

Catedrático de Derecho mercantil
Universitat Oberta de Catalunya
mpeguera@uoc.edu

1. INTRODUCCIÓN

Aparentemente, la Unión Europea ha culminado con éxito, por lo menos en términos políticos, su audaz apuesta regulatoria en materia de IA con la aprobación del Reglamento de Inteligencia Artificial (en adelante, RIA), publicado en el Diario Oficial el 12 de julio de 2024.[1] Con una tramitación larga

[1] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DO L, 2024/1689, 12.7.2024.

y compleja -algo habitual en instrumentos de este calado-, el RIA ha salido adelante y ha establecido un marco legal que aspira abiertamente a provocar de nuevo un 'efecto Bruselas' que lo convierta en modelo a seguir en otras jurisdicciones,[2] como ya ocurrió con el Reglamento General de Protección de Datos (RGPD).[3] Desde luego, éxitos pasados no garantizan éxitos futuros y nada asegura que el RIA vaya a lograr un reconocimiento similar. Entre otros motivos, porque en este caso el objeto de regulación difícilmente resiste una comparación con la protección de datos personales, un campo en el que la UE ya había acumulado una larga experiencia. Por una parte, experiencia legislativa, con diversas directivas, en especial la Directiva de 1995,[4] y con la consagración del derecho de protección de datos como derecho distinto al de privacidad en la Carta Europea de Derechos Fundamentales. Y por otra parte, también experiencia de aplicación judicial, con relevantes pronunciamientos del Tribunal de Justicia de la UE; así como experiencia de aplicación por las autoridades de protección de datos, junto con la reflexión, orientaciones y dictámenes del Grupo del Art. 29.[5] Todos estos precedentes hicieron posible alumbrar en 2016 una norma como el RGPD, que si bien ha alcanzado un notable predicamento global, suscita también críticas y no faltan voces que urgen a su reforma.

Ese caudal de experiencia regulatoria y de aplicación que acompañó la gestación del RGPD está ausente en el caso de la inteligencia artificial. Más aún: tratándose establecer un marco jurídico para la IA, el propio objeto de regulación resulta movedizo y de difícil aprehensión, a pesar de los intentos de definición. Con un objeto por naturaleza disruptivo y de contornos cambiantes, el legislador se enfrenta a un reto mayúsculo y bien se le puede aplicar la metáfora de la justicia ciega: aquí no en el sentido de aplicar el Derecho sin prejuicios, sino en el sentido de legislar con los ojos vendados por la imposibilidad de avizorar cabalmente las características del fenómeno que se dispone a regular, o por lo menos, los rasgos que este fenómeno puede presentar en el futuro más inmediato, por no hablar ya de los que puede revestir a medio plazo.

---

[2] Así, el Consejo Europeo se fijó como objetivo que la UE "sea un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética". Vid. Consejo Europeo, *Conclusiones de la Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020)*, EUCO 13/20, 2020, p. 6.

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1-88

[4] La hoy derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31-50.

[5] Hoy Comité Europeo de Protección de Datos (cfr. art. 68 del RGPD).

En estas condiciones, el riesgo de obsolescencia normativa es muy elevado. Ello explica que el RIA contenga numerosas remisiones a futuros desarrollos y concreciones que se confían a la Comisión Europa, a las entidades clave en la estructura de gobernanza que dibuja el propio Reglamento, así como a los organismos europeos de normalización que van a tener un papel fundamental en la traducción a estándares los requisitos previstos en el RIA.

Una muestra ilustrativa del carácter ineludiblemente provisional del enfoque regulatorio se puso de manifiesto en la necesidad de reaccionar con urgencia ante tras el lanzamiento de ChatGPT en noviembre de 2022, que hizo evidente el papel de los grandes modelos de lenguaje (LLM), aptos para múltiples propósitos prácticos. Se trataba de algo que el texto del Reglamento propuesto por la Comisión poco más de un año y medio antes, en abril de 2021, no había sido capaz de anticipar, de modo que tanto el Consejo como el Parlamento se apresuraron a formular enmiendas para acoger modelos y sistemas de propósito general, frente al esquema inicial de la propuesta, que se centraba en sistemas previstos para finalidades específicas.

Todo ello no significa que el RIA haya surgido de la nada. Estuvo ciertamente precedido por múltiples estudios y trabajos. Pero siempre en un marco de incertidumbre sobre el modo en que el legislador debía actuar ante el imparable desarrollo de las tecnologías de IA. En un escenario así, regular comporta el riesgo de llegar *demasiado pronto* y comprometer con trabas legislativas el desarrollo de la IA, la innovación y la efectiva adopción de sistemas de IA en la UE. A la vez, la eventual decisión de diferir la intervención legislativa a la espera de comprobar cómo se desarrolla este fenómeno implica el riesgo de llegar *demasiado tarde*, cuando quizás ya no es posible reconducir algunos de los efectos negativos consolidados.

En este contexto, el legislador ha adoptado en el Reglamento varias decisiones clave. Una de ellas es la de enfocar la regulación desde la lógica de la seguridad de productos, un campo en el que la UE goza ciertamente de una larga experiencia, pero cuya aptitud para abordar el complejo fenómeno de la IA no resulta evidente.

Otra de las decisiones esenciales de política jurídica ha consistido en construir un régimen jurídico enfocado a eliminar o mitigar los potenciales riesgos del empleo de sistemas de IA. Esta óptica del riesgo -de los peligros que los sistemas de IA pueden representar para la salud, la seguridad y los derechos consagrados en la Carta Europea de Derechos Fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente en la Unión Europea-[6] permite al legislador sostener que la intervención normati-

[6] Cfr. Art. 1 RIA.

va se limita a ofrecer salvaguardas frente los riesgos más graves -en ocasiones llegando a la prohibición total de ciertas prácticas de IA-, sin ir más allá de lo estrictamente necesario para este propósito y dejando un amplio margen de libertad para el desarrollo, comercialización y utilización de sistemas que no comporten tales peligros.

La lectura del RIA desde la óptica del riesgo permite interpretarlo como un texto que establece diversos conjuntos de requisitos y obligaciones en atención al nivel de riesgo que plantea la introducción en el comercio, puesta en servicio y utilización de sistemas de IA, y que varían en función de sus capacidades, finalidad, y ámbito en el que se emplean. Aunque no se trata de una perfecta gradación, distinguimos fácilmente entre un grupo de usos o prácticas de IA que se declaran prohibidas, por revestir un nivel de riesgo potencial excesivo o inaceptable, y un grupo de supuestos de riesgo alto, al que se destinan la mayor parte de las previsiones del texto. Por otra parte, se fijan obligaciones para los llamados modelos de uso general, con obligaciones particulares en los casos en que estos modelos plantean riesgos sistémicos. Finalmente, se identifican ciertos sistemas que por sus características particulares -la confusión o desinformación que pueden provocar a personas que desconocen que se hallan ante actividades desarrolladas, o contenidos generados, por IA- quedan sujetos a ciertas obligaciones de transparencia e información. En rigor, no se trata de sistemas de "riesgo limitado", ya que estos mismos sistemas pueden ser, a su vez, sistemas de alto riesgo, en cuyo caso deberán cumplir los correspondientes requisitos de modo cumulativo.

La delimitación del catálogo de prácticas prohibidas, y de aquellas que se consideran de alto riesgo y sujetas por tanto a un gravoso conjunto de exigencias regulatorias, es un punto de partida que adopta el legislador confiando en algunos estudios y análisis preliminares. Esta clasificación, sin embargo, no parece completamente ajena a ciertos apriorismos, ni a las influencias ejercidas por la industria y por el activismo civil y está llamada a sufrir modificaciones. A su vez, el propio RIA arbitra la posibilidad de que, en el caso concreto, un sistema subsumible en la relación ámbitos y casos de alto riesgo, pueda escapar a esta calificación si resulta suficientemente justificado, a partir de determinados criterios, que el nivel de riesgo que plantea es de carácter menor.

2. LA PERSPECTIVA DEL RIESGO

El *iter* legislativo del RIA se inicia formalmente con la publicación de la Propuesta de Reglamento por parte de la Comisión, el 21 de abril de

2021,[7] que viene a recoger la estela de los trabajos previos. Así, en abril de 2018, la Comisión publicó su comunicación *Inteligencia artificial para Europa.*[8] En diciembre del mismo año, preparó un *Plan coordinado sobre la inteligencia artificial*,[9] y en abril de 2019, hizo pública una nueva comunicación, titulada *Generar confianza en la inteligencia artificial centrada en el ser humano.*[10] También en 2019, el Grupo de expertos de alto nivel sobre IA, nombrado por la Comisión el año anterior, elaboró unas *Directrices éticas para una IA fiable.*[11] Poco más tarde, la Comisión elaboró el *Libro Blanco sobre la inteligencia artificial*, publicado en febrero de 2020.[12] Por su parte, el Parlamento Europeo dictó una Resolución en octubre de 2020 sobre aspectos éticos de la IA, que recomendaba a la Comisión presentar una propuesta de instrumento legislativo para la regulación de la IA, incluyendo una detallada propuesta de texto articulado.[13] Estos trabajos condujeron a la publicación de la propuesta de Reglamento de abril de 2021, que vino acompañada por los habituales documentos de evaluación del impacto de la misma.[14]

La justificación que se aportó para la intervención legislativa se refiere esencialmente a los problemas relacionados con el uso de los sistemas de IA y con las consecuencias de la ausencia de normativa armonizada en la materia. Tales problemas son, de un lado, los riesgos que se derivan del uso de la IA, particularmente en términos de salud, seguridad, y derechos fundamentales y valores de la UE. Por otra parte, la falta de seguridad jurídica en un campo no regulado y no armonizado. Esta falta de regulación lleva a una falta de confianza en la IA que perjudica el desarrollo de esta tecnología en Europa y reduce la competitividad de la UE. Esto exige una intervención al nivel de la

---

[7] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021, COM(2021) 206 final.

[8] Bruselas, 25.4.2018, COM(2028) 237 final.

[9] Bruselas, 7.12.2018, COM(2018) 795 final.

[10] Bruselas, 8.4.2019, COM(2019) 168 final.

[11] Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, *Directrices éticas para una IA fiable*, Oficina de Publicaciones, 2019, https://data.europa.eu/doi/10.2759/14078.

[12] Comisión Europea, *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final.

[13] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html.

[14] *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final.

UE, ya que las medidas que pudieran adoptar aisladamente los Estados miembros comportarían una indeseable fragmentación del mercado.[15]

En lo referido concretamente a la seguridad de productos, el marco legal en vigor se halla integrado por normas de carácter transversal, como el Reglamento (UE) 2023/988 de 10 de mayo de 2023 relativo a la seguridad general de los productos,[16] que sustituye a la Directiva anterior; o el Reglamento 2019/1020 de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos.[17] Se integra también por disposiciones sectoriales, como la Directiva sobre las Máquinas,[18] que a partir del 20 de enero de 2027 quedará sustituida por el nuevo Reglamento relativo a las máquinas;[19] el Reglamento sobre productos sanitarios;[20] o el Reglamento de seguridad de vehículos.[21]

Este marco normativo sobre seguridad resulta insuficiente para abordar los riesgos asociados al uso de la IA en productos. Por una parte, los riesgos que suscitan los productos físicos son distintos de los que plantea la IA: por

---

[15] Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Brussels, 21.4.2021 SWD(2021) 84 final (Part 2), pp. 13-30.

[16] Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo, DO L 135 de 23.5.2023, p. 1-51.

[17] Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.° 765/2008 y (UE) n.° 305/2011, DOUE L 169, 25.6.2019, p. 1-44.

[18] Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (refundición) DOUE L 157, 9.6.2006, p. 24-86, modificada en diversas ocasiones.

[19] Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo, *DO L 165 de 29.6.2023, p. 1-102*.

[20] Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.° 178/2002 y el Reglamento (CE) n.° 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo, DOUE L 117, 5.5.2017, p. 1-175, varias veces modificado.

[21] Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) 78/2009; (CE) 79/2009; y (CE) 661/2009 del Parlamento Europeo y del Consejo; y los diversos Reglamentos de la Comisión, DOUE L 325, 16.12.2019, p. 1-40, con diversas modificaciones ulteriores.

ejemplo, peligros vinculados a los sesgos presentes en los datos utilizados para entrenar modelos o diseñar algoritmos; problemas relacionados con la interpretación errónea de información en situaciones complejas; o efectos negativos que pueden repercutir en personas y bienes. Además, los riesgos pueden verse agravados por ataques externos que alteren los datos de entrada, a menudo de manera imperceptible, provocando fallos en el sistema. Por otra parte, la normativa vigente tampoco es adecuada porque, aunque cubre los riesgos derivados del software que actúa como componente de seguridad en productos, no contempla, más que en escasas excepciones, el software en sí mismo, ya sea el utilizado en servicios o el que se incorpore al producto tras su comercialización. Y en los supuestos en que el software sí está regulado, no se imponen requisitos suficientes para afrontar los riesgos propios de un sistema de IA, ni se considera la evolución continua de estos sistemas a lo largo del tiempo.[22]

La constatación de los problemas apuntados y de las insuficiencias de la legislación vigente, junto con la consideración de diversas opciones de política jurídica, llevaron a la Comisión a proponer un Reglamento de alcance horizontal, teniendo en cuenta el nivel de riesgo que puede plantear el uso de la IA en diversos contextos.

Tanto el *Libro Blanco sobre la inteligencia artificial* [23] como las recomendaciones del Parlamento Europeo,[24] ambos ya citados, sugirieron adoptar un enfoque basado en el riesgo, con el objetivo de limitar la regulación a los casos de uso de la IA en los que la salud, la seguridad y los derechos fundamentales de los ciudadanos puedan verse más gravemente amenazados. En particular, en el Libro Blanco la Comisión consideró necesario seguir un enfoque basado en el riesgo para alcanzar un equilibrio que evite una carga desproporcionada a los actores implicados, en especial a las pymes. Esto requiere, como reconocía la Comisión, disponer de criterios claros para distinguir entre distintas aplicaciones de IA y determinar si entrañan o no un riesgo alto. A este propósito, sugirió que una aplicación de IA debería considerarse de alto riesgo cuando concurran cumulativamente los dos criterios siguientes. Por una parte, que se emplee en un *sector* en el que, por sus características o por las

---

[22] Sobre esta percepción de la insuficiencia de la normativa de seguridad de productos, véase el *Impact Assessment* que acompaña la propuesta: *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final (Part 2), pp. 13-16.

[23] Comisión Europea: *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza,* Bruselas 19.02.2020, COM(2020) 65 final.

[24] *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020/2012(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html.

actividades que normalmente se llevan a cabo, resulte previsible la existencia de riesgos significativos. Por otra parte, que, además de emplearse en uno de los sectores identificados, el *uso concreto* del sistema de IA pueda dar lugar a riesgos elevados.[25] En sentido similar, el Parlamento Europeo recomendó un enfoque basado en el riesgo y orientado al futuro, con normas transversales para todos los sectores y normas sectoriales cuando sea preciso. Al igual que el Libro Blanco, indicó que sería necesaria una lista exhaustiva y cumulativa de sectores de alto riesgo y de usos o fines de alto riesgo. Y que debería someterse a reevaluación periódica tanto la lista como la propia metodología de evaluación de riesgos.[26]

Con algunas variaciones, este enfoque centrado en el riesgo es el que adoptó la propuesta y pasó al texto del RIA finalmente aprobado. En los siguientes epígrafes examinamos sumariamente la calificación de los riesgos que lleva al RIA a fijar prohibiciones absolutas para determinadas prácticas y a establecer un régimen particular para los sistemas de alto riesgo, tanto los que se enmarcan en la normativa armonizada de seguridad de productos como los sistemas independientes; a establecer ciertas obligaciones de transparencia en relación con determinados sistemas, destinadas a minimizar riesgos específicos, así como a fijar requisitos particulares para los modelos de uso general que presentan riesgo sistémico.

3. LA PROHIBICIÓN DE PRÁCTICAS DE IA QUE IMPLICAN UN RIESGO EXCESIVO

El listado de prácticas prohibidas, fijado en el artículo 5 del RIA, experimentó notables cambios a lo largo de la tramitación legislativa, llegando finalmente a una relación más extensa de la contemplada en la propuesta inicial, y con un detallado conjunto de matices y excepciones, particularmente en relación con determinados usos de la IA por los poderes públicos en materia de seguridad.

Un primer grupo de prácticas prohibidas se refiere a usos manipulativos o engañosos y de explotación y control social, que se prohíben por resultar esencialmente contrarias a los valores de la UE y a los derechos fundamentales reconocidos en la Carta. Se trata, por una parte, de los sistemas que empleen

---

[25] Véase el *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, Bruselas 19.02.2020, COM(2020) 65 final, pp. 21-22.

[26] Véase *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020/2012(INL)), puntos 12 a 16.

técnicas subliminales que trasciendan la conciencia de una persona, o de técnicas deliberadamente manipuladoras o engañosas que persigan o produzcan el efecto de modificar sustancialmente el comportamiento de una persona o de un colectivo. Se requiere que tales técnicas mermen apreciablemente la capacidad para tomar una decisión informada e induzcan a tomar una decisión que de otro modo no habrían tomado. Además, se exige que con ello se provoque a esa persona o a otra, o a un colectivo, prejuicios considerables, o que, por lo menos, sea razonablemente probable ese resultado perjudicial.[27] En sentido similar, se prohíben los sistemas de IA que exploten alguna vulnerabilidad de una persona física o de un colectivo, que derivada de su edad, discapacidad o situación social o económica. De igual modo que en el caso anterior, el uso del sistema debe tener por objeto o por efecto alterar sustancialmente el comportamiento de la persona o personas afectadas, así como provocar perjuicios considerables a esa o a otra persona, o que tal perjuicio resulte razonablemente probable.[28]

En ambos casos, la prohibición se refiere a la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA de tales características. Resulta notable el cúmulo de requisitos que exige el RIA para prohibir estas prácticas, lo que reduce el alcance de la prohibición, además de plantear dificultades interpretativas. En sus considerandos, el RIA advierte que las técnicas de manipulación, sea subliminal o de otro tipo, menoscaban la autonomía personal sin que la persona afectada sea consciente de ello, y que incluso cuando es consciente de que se están empleando estas técnicas, la persona afectada puede seguir siendo engañada o no puede controlarlas u oponer resistencia.

Tendría sentido que el empleo de tales técnicas resultara ya prohibido con carácter general, pero el Reglamento exige además el resultado del daño, o su probabilidad razonable, tanto en el caso de manipulación como en el de explotación de vulnerabilidades. Daño o perjuicio que puede ser de todo tipo, al haberse prescindido en el texto final de la caracterización establecida en la propuesta inicial, que exigía perjuicio de carácter físico o psicológico.

El alcance de ambas prohibiciones queda en cierto modo matizado por las indicaciones del considerando 29. En este se advierte que «no es necesario que el proveedor o el responsable del despliegue tengan la intención de causar un perjuicio considerable, siempre que dicho perjuicio se derive de las prácticas de manipulación o explotación que posibilita la IA». Al mismo tiempo se advierte que no puede presuponerse que existe la intención de alterar el comportamiento si tal alteración resulta de factores externos al sistema de IA, que ni el provee-

[27] Art. 5.1.a) RIA.
[28] Art. 5.1.b) RIA.

dor ni el responsable del despliegue controlan ni están en condiciones de mitigar -aunque conviene recordar que conforme al tenor del art. 5, en ninguno de los casos es necesaria tal intención sino que basta con que el sistema produzca el efecto de la alteración sustancial del comportamiento-. En sentido similar se advierte de que las prácticas comerciales comunes y legítimas, por ejemplo en el campo de la publicidad, que cumplan con el ordenamiento en vigor, no deben considerarse en sí mismas prácticas de manipulación perjudiciales. A este respecto, las conductas recogidas en estas prohibiciones ya estaban parcialmente contempladas, aunque no referidas de modo concreto a la IA, en la regulación sobre prácticas comerciales desleales.[29]

El RIA opta también por prohibir de la introducción en el comercio, puesta en servicio o utilización de ciertos sistemas de IA de *social scoring* o "puntuación ciudadana". En particular, se prohíben aquellos que se destinan a evaluar o clasificar a personas físicas o colectivos a lo largo de un cierto tiempo a partir de su comportamiento social o de "características personales o de su personalidad conocidas, inferidas o predichas", y siempre que la puntuación resultante provoque alguna de las situaciones que contempla el precepto. Se trata específicamente de que ocasione un trato perjudicial o desfavorable "en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente"; o bien un trato perjudicial o desfavorable para las personas afectadas, "que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este". Del tenor del precepto cabría colegir que si el trato perjudicial, o incluso meramente desfavorable, se produce en el mismo contexto en el que se recabaron los datos -por ejemplo el lugar de trabajo- el sistema no quedaría afectado por la prohibición, salvo que el trato resulte a su vez injustificado o desproporcionado. Por otra parte, no se proporcionan elementos para valorar el carácter injustificado o desproporcionado, a la vez que se da a entender que ese perjuicio podría resultar aceptable si guarda proporción con el comportamiento social observado, cuestión que suscita algunos interrogantes.

---

[29] En este sentido, el considerando 29 RIA expone que la prohibición complementa lo dispuesto en la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior (DOUE L 149, 11.6.2005). Como apuntaron VEALE y BORGESIUS en relación con la propuesta de reglamento, la prohibición de este tipo de conductas de manipulación se estaba ya prevista el artículo 5 de la Directiva 2005/29/CE que considera desleal la práctica contraria a los requisitos de la diligencia profesional que "distorsiona o puede distorsionar de manera sustancial, con respecto al producto de que se trate, el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica, o del miembro medio del grupo, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores", grupo que puede caracterizarse por ser consumidores especialmente vulnerables por padecer una dolencia física o un trastorno mental o por su edad o su credulidad. *Vid.* Michael VEALE, Frederik BORGESIUS, "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International* (2021) 22(4) 97-112, esp. p. 99.

El supuesto -como ocurre con muchos otros- plantea la dificultad de fijar las fronteras de la práctica prohibida. A diferencia de los casos de manipulación o de explotación de vulnerabilidades, aquí no se hace referencia a la aptitud en abstracto para provocar un prejuicio (probabilidad razonable), sino que incluye como parte de la definición del sistema cuyo uso se busca prohibir el hecho de que este provoque efectivamente el trato perjudicial o desfavorable antes mencionado. Tratándose de una circunstancia que sólo cabe apreciar *a posteriori*, la delimitación de la conducta prohibida parece poco afortunada y por tanto de escasa seguridad jurídica. No ayudan a una mejor precisión las observaciones del considerando 31, que señala que "deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación *y den lugar a* esos resultados perjudiciales o desfavorables", y que a su vez advierte que la prohibición "no debe afectar a prácticas lícitas de evaluación de las personas físicas que se efectúen para un fin específico de conformidad con el Derecho de la Unión y nacional".[30]

Se consideran también sistemas de IA de riesgo excesivo, y en consecuencia se prohíbe su introducción en el mercado, su puesta en servicio para este fin y su uso, los destinados a predecir el riesgo de que una persona comenta un delito a partir únicamente de su perfil o de la evaluación de su personalidad,[31] un supuesto no previsto en la propuesta inicial y que se acabó de concretar durante la negociación interinstitucional en los trílogos.[32] La prohibición se fundamenta en la presunción de inocencia, en virtud de la cual las personas deben ser juzgadas basándose en su comportamiento real y no a partir de predicciones realizadas por un sistema de IA de estas características.[33] La prohibición alcanza sólo a predicciones basadas únicamente en la elaboración de perfiles o en la evaluación de los rasgos y características de la personalidad. Esto parece apuntar al hecho de que no haya habido una valoración humana, y así lo viene a sugerir el considerando 42. Aunque no se hace explícito en la norma, parece claro que se tienen en cuenta los riesgos discriminatorios de este tipo de sistemas predictivos, que pueden perjudicar a determinados individuos a consecuencia de los sesgos de los datos de entrenamiento.

Se excluyen expresamente de la prohibición los sistemas de IA utilizados para apoyar la valoración humana sobre la participación de una persona en una actividad delictiva, con base en hechos objetivos y verificables.[34] De acuer-

---

[30] Cdo. 31 RIA.

[31] Art. 5.1.d) RIA.

[32] Cabe notar, por otra parte, que la redacción final no incluye la predicción de incurrir o reincidir en infracciones administrativas, que había sido contemplada en las enmiendas del Parlamento de 14 de junio de 2023.

[33] Cdo. 42 RIA.

[34] Art. 5.1.d) RIA.

do con el considerando 42, esta prohibición no alcanza a los análisis de riesgos «que *no estén basados* en la elaboración de perfiles de personas o en los rasgos y características de la personalidad de las personas», y apunta como ejemplos el caso de los sistemas que evalúan la probabilidad de fraude financiero por parte de empresas a partir de transacciones sospechosas, o la probabilidad de localización de mercancías ilícitas por parte de autoridades aduaneras.[35]

El reconocimiento facial ha sido un punto controvertido en la tramitación del Reglamento y finalmente se ha incluido una prohibición general de los sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción indiscriminada de imágenes de internet o de circuitos cerrados de televisión como las cámaras de seguridad. El fundamento alegado en este caso es la contribución de estos sistemas al agravamiento de la sensación de vigilancia masiva, y a su impacto en los derechos fundamentales, particularmente en el derecho a la intimidad.[36]

Particularmente novedosa resulta la prohibición de sistemas de IA para inferir emociones en el lugar de trabajo o en centros educativos.[37] Diversas organizaciones habían solicitado una prohibición absoluta de estos sistemas, que finalmente se limitó a su uso en el ámbito de las relaciones de trabajo y en el campo de la educación, y contó con la pública oposición de parte de la industria, alegando los efectos beneficiosos que pueden reportar estas tecnologías. El fundamento expresado para esta prohibición se sitúa en las dudas que generan la fiabilidad y la base científica para la detección o deducción de emociones, que se manifiestan de modo diverso en distintas culturas y colectivos y que pueden conducir a resultados discriminatorios. El motivo para confinar la prohibición al ámbito laboral y educativo radica en que en estos contextos se da un desequilibrio de poder, que viene a añadirse al carácter intrusivo de estos sistemas. Se excluyen del ámbito de la prohibición aquellos sistemas que tengan fines exclusivamente médicos o de seguridad, lo que no parece referirse a la exclusión de sistemas de detección de dolor o cansancio a fin de evitar accidentes, pues el considerando 18 ya excluye estos objetivos de la propia noción de reconocimiento de emociones.[38]

---

[35] Cdo. 42 RIA.

[36] Art. 5.1.d) RIA y Cdo. 43 RIA.

[37] Art. 5.1.f). Por "sistema de reconocimiento de emociones" se entiende, a efectos del Reglamento, «un sistema de IA destinado a distinguir o inferir las emociones *o las intenciones* de las personas físicas a partir de sus datos biométricos», vid. Art. 3.39) RIA.

[38] En efecto, el Considerando 18 precisa que «[e]l concepto [de reconocimiento de emociones] se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se

Por último, la biometría se halla en el centro de otros dos grupos de prohibiciones. Por una parte, se prohíben los sistemas que clasifican individualmente a las personas por sus datos biométricos para deducir o inferir datos sensibles como la raza, preferencias políticas o sindicales, convicciones religiosas o filosóficas, o la vida y orientación sexual. El precepto advierte que «esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho», lo que plantea de nuevo la cuestión de las fronteras del supuesto de hecho al que se aplica la prohibición. Por otra parte, se prohíben los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley (*law enforcement*), con una serie de excepciones. Se trata de un punto objeto de controversia y grandes esfuerzos de negociación, por el interés de los Estados en disponer de herramientas de este tipo para su actividad de control y cumplimiento de la ley. La norma recoge tres excepciones, que se refieren a los casos en que el uso de esta tecnología resulte estrictamente necesario para la búsqueda selectiva de víctimas de ciertos delitos y de personas desaparecidas; para prevenir amenazas inminentes contra la vida o seguridad y de amenazas reales y o previsibles de atentado terrorista; o para localizar o identificar a un sospechoso de determinados delitos, recogidos en el Anexo II del Reglamento.[39]

4. SISTEMAS DE IA DE ALTO RIESGO VINCULADOS A LA LEGISLACIÓN ARMONIZADA SOBRE SEGURIDAD DE PRODUCTOS

Como señalamos en la introducción, junto con la decisión de adoptar una perspectiva que atiende al riesgo, el legislador europeo tomó también la decisión de insertar la regulación, en la medida de lo posible, en el marco de la normativa de seguridad de productos, considerando que muchas de las soluciones de IA van a estar vinculadas a productos para los que ya existe regulación sectorial de seguridad. En este sentido, el RIA busca aprovechar este bloque de normativa armonizada para encajar en ella los nuevos requisitos que se van a requerir a los sistemas de IA vinculados a los productos cubiertos por dicha legislación.

---

utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro».

[39] Las excepciones a esta prohibición se rodean de precisas cautelas y salvaguardas que el RIA prevé en los apartados 2 a 7 del artículo 5.

Ese conjunto de normas de seguridad de productos se divide en dos grupos, según se trate de disposiciones dictadas conforme al llamado "nuevo marco legislativo para la comercialización de productos",[40] establecido en 2008, o bien se trate de normas armonizadas anteriores. Entre las dictadas al amparo del nuevo marco legislativo se incluyen, entre otras, normas referidas a juguetes, máquinas, embarcaciones, ascensores, equipos radioeléctricos, equipos a presión o productos sanitarios. Entre las normas anteriores se hallan disposiciones sobre vehículos de motor, aviación civil, equipos marinos o sistema ferroviario, entre otros.[41]

En el contexto de esta legislación armonizada de seguridad de producto, y más específicamente en el marco del listado de disposiciones concretas de esa legislación que recoge el Anexo I, el RIA considera que son sistemas de AI de alto riesgo aquellos que constituyan, en sí mismos, un producto de los contemplados en esta legislación sectorial -o estén destinados a ser utilizados como componente de seguridad de estos productos-, siempre que, conforme a dicha legislación sectorial, el producto o el componente deba someterse a una evaluación de conformidad realizada por un organismo independiente. Se busca así integrar las normas del RIA en el marco de la legislación sectorial ya existente en materia de seguridad, para garantizar la coherencia y evitar duplicidades y cargas excesivas. De esta forma, los requisitos exigidos RIA se comprobarán en general como parte de los procedimientos de evaluación de conformidad previstos en las disposiciones del "nuevo marco legislativo", con

---

[40] El "nuevo marco legislativo" (*New Legislative Framework* o *NLF*) al que se refiere la Propuesta de Reglamento IA se estableció mediante dos disposiciones dictadas el 9 de julio de 2008. Por una parte, la Decisión 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo, (DO L 218 de 13.8.2008, p. 82), que ofrece un modelo para la elaboración de normas sectoriales sobre seguridad y comercialización de productos en la UE. Y, por otra parte, el Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) 339/93 (DO L 218 de 13.8.2008, p. 30). Este Reglamento 765/2008 fijó los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos, si bien la parte referida a la vigilancia del mercado se suprimió para quedar regulada en el más reciente Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) 765/2008 y (UE) 305/2011 (DOUE L 169 de 25.6.2019, p. 1). La Comisión se ha planteado la conveniencia de reformar este "nuevo marco legislativo", para lo que puso en marcha un proceso de evaluación para valorar su efectividad, eficiencia y relevancia, y en particular, entre otros aspectos, si sigue siendo útil para tratar sobre la seguridad de los productos que pueden experimentar cambios a lo largo de su ciclo de vida, como los productos inteligentes conectados, o también para valorar si fijar físicamente el marcado CE y otra información en el propio producto sigue siendo adecuado (véase el documento *Commission Staff Working Document Evaluation of the New Legislative Framework*, Brussels, 16.11.2022 SWD(2022) 364 final/2).

[41] Vid. Anexo I, RIA.

la posibilidad de fijar algunos requisitos específicos sobre la integración del sistema de IA en el producto. Así, el RIA viene a complementar esa normativa sectorial para afrontar los riesgos de la IA.

Además el RIA contempla un catálogo casos de sistemas de IA independientes -en el sentido de no vinculados a esta normativa sectorial de seguridad de productos- a los que asigna también la calificación de sistemas de alto riesgo, y a los que hacemos referencia a continuación.

5. SISTEMAS DE IA DE ALTO RIESGO INDEPENDIENTES

Siguiendo las orientaciones del Libro Blanco,[42] y de la recomendación del Parlamento Europeo,[43] a las que hemos hecho referencia más arriba, el Reglamento identifica una serie de sectores o ámbitos en los que se considera probable que el uso de la IA ocasione riesgos elevados y, dentro de cada uno de estos ámbitos, ciertos supuestos de uso específicos. De este modo, califica como sistemas de alto riesgo -además de los ya señalados por su vinculación a la normativa armonizada- aquellos sistemas que quedan recogidos en el listado de supuestos de sistemas de IA de alto riesgo que se contiene en el Anexo III del propio Reglamento.[44]

Para elaborar este listado inicial en la propuesta de Reglamento -listado que la Comisión podrá modificar ulteriormente dentro de ciertos límites-, la Comisión siguió una metodología que tiene en cuenta si el sistema de IA en cuestión y su uso previsto genera un riesgo elevado para la salud o seguridad, o para los derechos y libertades fundamentales de las personas, aplicando una serie de criterios que se relacionan en los trabajos preparatorios.[45] Para este análisis tuvo en cuenta, entre otros, los casos de riesgo ya apuntados en el informe del Parlamento Europeo,[46] así como tipos de usos identificados en múl-

---

[42] Vid. *Libro Blanco sobre la inteligencia artificial*, cit., apartado 5.C, pp. 21-22.

[43] *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020/2012(INL)).

[44] Art. 6.2 RIA.

[45] Véase el apartado 5.3 del documento de evaluación de impacto de la propuesta, en particular la nota 232 (p. 50) (en la primera parte del documento) y el Anexo 5.4 (en la segunda parte del documento): *Commission Staff Working Document. Impact Assessment. Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Brussels, 21.4.2021 SWD(2021) 84 final (Partes 1 y 2).

[46] *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020/2012(INL).

tiples estudios.[47] Los criterios para la evaluación llevada a cabo -criterios que la Comisión considera objetivos y no discriminatorios, en la medida en que tratan de modo similar los sistemas de IA similares, sin distinguir en función de su origen dentro o fuera de la UE- contemplan, entre otros aspectos, en qué medida el sistema de IA se ha utilizado o se va a utilizar; si ha causado daños a la salud, seguridad o derechos y libertades fundamentales de las personas o ha generado preocupación seria de su posible materialización; el alcance del impacto negativo de los daños y la posibilidad de afectar negativamente a una pluralidad o grupos enteros de personas; la medida en que las personas potencialmente afectadas dependen del resultado producido por el sistema -por ejemplo, si pueden o no rechazar que se les aplique-, o se hallan en una posición vulnerable frente al usuario del sistema de IA; en qué medida el resultado del sistema IA puede revertirse; si existen remedios legales efectivos; y hasta qué punto la vigente legislación de la UE es capaz de impedir o minimizar los riesgos potenciales del sistema de IA.[48]

Como resultado de este análisis, la Comisión identificó en su propuesta inicial una serie de sectores y casos de uso específicos. El listado de sectores o ámbitos se ha mantenido de modo esencialmente invariado en el texto final del RIA. Concretamente, los sectores incluidos en el Anexo III del RIA son los siguientes: (1) Biometría (en la medida en que su uso esté permitido); (2) Infraestructuras críticas; (3) Educación y formación profesional; (4) Empleo, gestión de los trabajadores y acceso al autoempleo; (5) Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones; (6) Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; (7) Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; y, por último, (8) Administración de justicia y procesos democráticos. Dentro de cada uno de estos ocho ámbitos se señalan determinados usos de sistemas de IA que reciben la calificación de riesgo alto.

---

[47] Entre otros muchos materiales, se incluyen el informe de ISO sobre casos de uso de IA: *AI Use Cases* (ISO/IEC TR 24030), https://www.iso.org/standard/77610.html; datos derivados de la preparación del informe *Directrices éticas para una IA fiable*, publicado por el High-Level Expert Group On Artificial Intelligence (HLEG), 2019, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines; resultados de la consulta pública llevada a cabo con ocasión del *Libro Blanco: la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza,* Bruselas 19.02.2020, COM(2020) 65 final; etc.

[48] Vid. *supra*, nota 45.

5.1. Ejemplos de casos de uso relevantes

El Anexo III especifica casos de usos dentro de cada uno de los ámbitos referidos, de los que destacaremos sólo algunos ejemplos, con especial mención de las novedades que el texto final incluyó respecto de la propuesta inicial.

Así, en el caso de la biometría se califican como de riesgo alto, los *sistemas de identificación biométrica remota*. Naturalmente, deben entenderse excluidos aquellos sistemas que se hallan prohibidos por aplicación del artículo 5.1.h), referidos a la identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley, a los que ya hemos hecho referencia. La texto final del RIA matiza que incluye sólo los supuestos de identificación y no los de mera "verificación" o autenticación; esto es, los casos en que no se trata de "identificar" a una persona (averiguar quién es, a partir de contrastar sus datos biométricos con los almacenados en una base de datos de referencia),[49] sino que se busca simplemente de confirmar que esa persona es quien dice ser, comparando sus datos biométricos con los ya registrados como correspondientes a dicha persona.[50] Por su parte, la mera verificación -que puede tener como finalidad, por ejemplo, permitir el acceso a un servicio, desbloquear un dispositivo o facilitar la entrada a un recinto- queda fuera del supuesto de riesgo alto incluido en el listado.[51] Se incluyen también en la calificación de alto riesgo los sistemas de IA para la categorización biométrica en función de atributos o características *sensibles o protegidos*, basada en la *inferencia* de dichos atributos o características, así como los sistemas de *reconocimiento de emociones*. A este último respecto, cabe recordar que el reconocimiento de emociones en el ámbito laboral y en el ámbito educativo, por su especial potencial discriminatorio, se configuran como *prácticas prohibidas* en el artículo 5.

---

[49] El art. 3.35 RIA define la *identificación* biométrica como « el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos».

[50] El art. 3.36 RIA define la *verificación* biométrica como « la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente».

[51] Cabe apuntar que, desde el punto de vista de Protección de Datos, el Comité Europeo de Protección de Datos (CEPD) considera que tanto la identificación como la autenticación o verificación suponen un tratamiento de categorías especiales de datos. Véanse las *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, versión 2.0, de 26 de abril de 2023, disponibles en https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf. La Agencia Española de Protección de Datos, que inicialmente había mantenido un criterio distinto, se ha adaptado a la posición del CEPD en su *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, de noviembre de 2023, disponible en https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf.

En relación con las infraestructuras críticas, cabe destacar que la versión final del RIA añade los sistemas de IA destinados a ser empleados como componentes de seguridad en la gestión y funcionamiento de las infraestructuras digitales críticas, además de los supuestos ya contemplados en la propuesta inicial sobre el tráfico rodado o del suministro de agua, gas, calefacción o electricidad.

En el campo de la educación y la formación profesional, la versión final del RIA añade matices, si bien lo esencial sigue siendo el uso de sistemas de IA para determinar el acceso a centros de formación y para evaluar a los alumnos y determinar los niveles formativos a los que podrán acceder. Quizás de modo más significativo se añaden como caso de riesgo alto los sistemas destinados a ser utilizados para detectar fraude en los exámenes, fraudes que ciertamente se han visto impulsados con la irrupción de las herramientas de IA generativa.

En el ámbito laboral, el texto final mantiene en lo esencial la determinación como casos de riesgo alto de los sistemas empleados para la contratación o selección de personal, con particular énfasis en la publicación de anuncios de empleo específicos y el filtrado y evaluación de solicitudes y candidatos, así como los sistemas utilizados en la evaluación del rendimiento, y toma de decisiones sobre condiciones laborales y asignación de tareas. En este último punto, la versión final destaca que se trate de asignación de tareas a partir de comportamientos individuales o rasgos o características personales.

En cuanto a los sistemas empleados para el acceso a servicios públicos y privados esenciales y para permitir el disfrute de los mismos, la versión final del RIA pone mayor énfasis en que también los servicios públicos deben ser de carácter esencial, y entre ellos incluye los de asistencia sanitaria. Cuando se trata de sistemas para evaluar la solvencia de personas físicas o establecer su calificación crediticia,[52] la versión final elimina la excepción referida a los sistemas de IA puestos en servicio por parte de proveedores a pequeña escala para su uso propio, mientras que exceptúa de la calificación de alto riesgo el caso de los sistemas para detectar fraudes financieros. Por otra parte, añade el caso de los sistemas para evaluar riesgos y fijar precios de seguros de vida y salud.

Por lo demás se introducen variaciones en los casos de uso referidos a sistemas de IA para fines de aplicación de la ley, para migración, asilo y gestión de fronteras -excluyendo la verificación de documentos de viaje-, o para propósitos de administración de justicia y procesos democráticos. En este último ámbito se añaden como casos de alto riesgo los sistemas «para influir en el resultado de una elección o referéndum o en el comportamiento electoral de

[52] Este tipo de sistemas puede presentar un cierto solapamiento con las prácticas que son objeto de prohibición en el art. 5.1.c) sobre *social scoring* al que nos hemos referido más arriba.

personas físicas que ejerzan su derecho de voto en elecciones o referendos», algo que naturalmente debe considerarse a la luz de las prácticas prohibidas sobre manipulación y que debe entenderse sin perjuicio del recientemente aprobado Reglamento (UE) 2024/900, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política.

5.2. Criterios para rechazar la calificación de riesgo alto

A diferencia de lo previsto en la propuesta inicial, el texto final del RIA admite que pueda considerase que un determinado sistema de IA, a pesar aparecer incluido en el listado de casos del Anexo III, no es de alto riesgo, y que en consecuencia no rijan los requisitos y obligaciones que prevé el Reglamento para los sistemas de alto riesgo. Así, se prevé expresamente que «un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones» (art. 6.3 RIA).[53]

Con ello se trata de evitar una catalogación automática como sistema de alto riesgo, que podría resultar desproporcionada en el caso concreto. En efecto, el catálogo del Anexo III no es más que una aproximación, que difícilmente puede asegurar que en todas las situaciones contempladas se producirá una situación efectiva de riesgo alto. En especial, el Reglamento considera que un sistema *no plantea tal riesgo* cuando no influye sustancialmente en el resultado de la toma de decisiones, es decir, que «no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada»[54]. Y considera que este será el caso si se cumple *alguna* de las cuatro condiciones que recoge el artículo 6.3 RIA, y que son las siguientes.

---

[53] En una versión anterior, en lugar del adverbio "también" se empleaba la expresión "en particular", que resultaba más ajustada a la versión inglesa, que utiliza la expresión "including": «an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, *including* by not materially influencing the outcome of decision making». El sentido aparente es que la falta de influencia decisiva en el resultado de la decisión sería uno, entre otros, de los posibles factores que implicaría ausencia de riesgo alto del sistema. El considerando 53 señala que «pueden existir casos específicos en los que los sistemas de IA referidos en ámbitos predefinidos especificados en el presente Reglamento no entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, dado que no influyen sustancialmente en la toma de decisiones *o no perjudican dichos intereses sustancialmente*. A efectos del presente Reglamento, por sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones debe entenderse un sistema de IA que no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada» (énfasis añadido).

[54] Cfr. cdo. 53 RIA.

Primera: que el sistema de IA tenga por objeto llevar a cabo *una tarea de procedimiento limitada*. A este respecto, los considerandos ofrecen algunos ejemplos: un sistema que transforme datos no estructurados en datos estructurados; un sistema que clasifique en categorías los documentos recibidos; o un sistema que se utilice para detectar duplicados entre un gran número de aplicaciones.[55] El carácter concreto y restringido de la tarea hace que los riesgos que presenta el sistema sean limitados y que estos no aumenten por el hecho de que el sistema se emplee en uno de los ocho ámbitos considerados en el Anexo III.

Segunda: que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada. Se entiende que la mejora de esa actividad humana previa sólo puede comportar un riesgo menor.[56] Como ejemplos de este caso, los considerandos señalan los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos ya redactados -se entiende que por parte de humanos- a efectos de ajustarlo a un registro determinado, por ejemplo de carácter profesional o de naturaleza más académica, o bien para adaptarlo a una política de comunicación de marca.

Tercera: que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella. El hecho de que previamente haya tenido lugar una evaluación humana supone, a los ojos del RIA, que el riesgo del sistema no será elevado. Y apunta, como ejemplos, el uso para comprobar *a posteriori* si un profesor puede haberse desviado de su criterio general en la calificación de exámenes, o el uso para identificar otras anomalías o incoherencias en relación con decisiones previas.

Cuarta: que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el Anexo III. En este último caso lo que se considera es el riesgo que el uso de este sistema pueda representar para el resultado de la evaluación de un sistema de IA. Al limitarse a una tarea preparatoria, el Reglamento considera que su repercusión en la evaluación subsiguiente sería muy escasa desde el punto de vista del riesgo. Los ejemplos que proporcionan aquí los considerandos incluyen soluciones inteligentes para la gestión de archivos, así como sistemas de traducción de documentos.

Con independencia de estas cuatro condiciones, se dispone que en ningún caso se podrá excepcionar de su calificación como de alto riesgo aquellos

---

[55] Cfr. cdo. 53 RIA.

[56] Cfr. cdo. 53 RIA.

sistemas incluidos en el Anexo III que lleven a cabo la *elaboración de perfiles* de personas físicas, esto es, «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».[57]

A través de la adopción de actos delegados, la Comisión podrá modificar las condiciones citadas, así como añadir nuevas, «cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del Anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas».[58] Inversamente, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales en la Unión, la Comisión adoptará actos delegados para suprimir una o más de estas condiciones que permiten considerar que el sistema no es de riesgo alto.

De la redacción del precepto resulta que el hecho de que se verifique alguna de estas cuatro condiciones -o de las que en el futuro añada la Comisión- determina por sí mismo que el sistema de que se trate, incluido en el Anexo III, *no* es de alto riesgo. El establecimiento de este nuevo automatismo no deja de ser llamativo, toda vez que la verificación de si alguna de estas condiciones se cumple puede resultar dudoso en muchos casos. Esta valoración corresponde al proveedor del sistema de IA, a quien se le exigen determinados deberes de documentación y transparencia. Así, cuando el proveedor estime -basándose en alguna de las anteriores condiciones- que su sistema *no* es de alto riesgo, deberá documentar su evaluación antes de que el sistema sea introducido en el mercado o puesto en servicio; deberá registrarlo en la base de datos de la UE en la que se registran los sistemas de alto riesgo del Anexo III;[59] y deberá facilitar la documentación de la evaluación a solicitud de las autoridades nacionales competentes.[60]

Como en tantas otras materias complejas, el legislador acude al auxilio de la Comisión encomendándole que emita unas directrices que resuelvan las dificultades. Así, el RIA encarga a la Comisión que, previa consulta con el Comité Europeo de IA, elabore directrices que especifiquen la aplicación

---

[57] Véase el Reglamento (UE) 2016/679 (RGPD), art. 4.4; la Directiva (UE) 2016/680, art. 3.4; y el Reglamento (UE) 2018/1725, art. 3.5.

[58] Art. 6.6. RIA.

[59] Arts. 6.4, 49.2 y 71 RIA.

[60] Art. 6.4 RIA.

práctica del artículo 6, junto con -nada menos que- una lista *exhaustiva* de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.[61] El alcance de este mandato resulta por lo demás algo confuso pues, mientras que el artículo 6.5 RIA, al establecerlo, se refiere en general a especificaciones sobre "la aplicación práctica del presente artículo" -por tanto, de todo el artículo 6-, el considerando 53 se refiere a estas directrices como relativas exclusivamente a la aplicación práctica de las cuatro condiciones arriba apuntadas, por las que determinados sistemas, a pesar de estar incluidos en el Anexo III no se tendrán por sistemas de riesgo alto; es decir, sólo al apartado 4 del referido artículo 6.

5.3. Modificaciones de la relación de casos del Anexo III

El listado de casos de uso de sistemas de IA podrá ser modificado por la Comisión en virtud de la autorización para adoptar actos delegados que el RIA le concede en el artículo 7. Aunque esta habilitación es una buena muestra de la flexibilidad de una normativa que se desea resistente al paso del tiempo y de la evolución tecnológica, llama la atención que se establezca como requisito para añadir nuevos casos que estos se hallen incluidos en alguno de los ocho ámbitos de actividad ya reseñados (cfr. Art. 7.1.a). Esta limitación trasluce el propósito de garantizar que la normativa no exceda de lo estrictamente necesario, sin embargo puede ir en contra precisamente de la deseada adaptabilidad -por lo menos, sin una nueva intervención del legislador de la Unión-. La modificación podrá consistir también en suprimir casos concretos de la lista cuando la Comisión considere que ya no plantean riesgos significativos y no se reduzca con ello el nivel general de protección de la salud, la seguridad y los derechos fundamentales.

Para llevar a cabo estas modificaciones, la Comisión tendrá en cuenta una compleja serie de factores, entre los que se incluyen los posibles efectos beneficiosos del sistema de IA de que se trate.

6. OBLIGACIONES DE TRANSPARENCIA FRENTE A RIESGOS DE CONFUSIÓN

Ciertos sistemas de IA quedan sujetos a obligaciones de transparencia, con independencia de si los sistemas en cuestión resultan o no de alto riesgo.

[61] Art. 6.5 RIA.

No se trata pues, de un conjunto de obligaciones previsto para sistemas que ofrezcan un riesgo *inferior* a los de alto riesgo, como en ocasiones se ha presentado. Simplemente se trata de sistemas que, siendo o no de alto riesgo, pueden dar lugar a confusiones -especialmente en cuanto a la naturaleza de los resultados- que deben ser adecuadamente evitadas mediante una explicación transparente, para que resulte claro que son producto de la operación de un sistema de IA y no una creación o una actividad humana.

Estas obligaciones, dispuestas en el artículo 50, transparencia se establecen en relación con: (a) los sistemas de IA destinados a interactuar directamente con personas físicas; (b) aquellos que generen contenido sintético de audio, imagen, vídeo o texto; (c) los sistemas de reconocimiento de emociones y de categorización biométrica; (d) los que generen o manipulen contenidos de audio o vídeo que constituyan una ultrasuplantación o *deep fakes*; y (e) los que generen o manipulen texto que se publica para informar de asuntos de interés público.

En la interacción *directa* con personas físicas es esencial que la persona física sepa que no está interactuando con un ser humano sino con un sistema de IA. Por ello, el sistema deberá estar diseñado y desarrollado para que dichas personas estén informadas de este extremo. No obstante, se exceptúan los casos en que la interacción con un sistema de IA resulte evidente para una persona razonablemente informada, atenta y perspicaz.

Para los sistemas de IA generativa que den lugar a resultados en forma de audio, imagen, vídeo o texto, se exige al proveedor del sistema, con ciertas excepciones y teniendo en cuenta las circunstancias, que la información de salida esté marcada en un formato legible por máquina, y que sea posible detectar que ha sido generada o manipulada artificialmente.

Para los sistemas de reconocimiento de emociones o de categorización biométrica (siempre que no se hallen prohibidos), se exige a los responsables del despliegue informar a los afectados y tratar sus datos conforme al RGPD. También se imponen obligaciones de transparencia a los responsables del despliegue de sistemas de IA que generen o publiquen imágenes, audio o vídeo, que constituya un *deep fake* (ultrasuplantación). En concreto se les exige hacer público que esos contenidos o imágenes han sido generados o manipulados de manera artificial. La obligación se suaviza en los casos en que el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción, donde se establece que declaración se hará de modo que no dificulte la exhibición o disfrute de la obra. Cuando el contenido generado o manipulado sea texto que se publique con el fin de informar sobre asuntos de interés público, los responsables del despliegue deberán divulgar su naturaleza artificial, aunque esto no será preciso si el contenido ha sido

posteriormente revisado por un humano, y cuando una persona física o jurídica asuma la responsabilidad editorial de la publicación.

También en este campo se prevé la elaboración de códigos de buenas prácticas bajo los auspicios de la Oficina de IA.

7. RIESGOS SISTÉMICOS DE LOS MODELOS DE USO GENERAL

Nos referimos, por último, a la consideración del riesgo sistémico que se incluye en la regulación de los llamados modelos de uso general. Como se indicó más arriba, la propuesta inicial del RIA estaba marcada por el enfoque a casos de uso específicos para determinar el nivel de riesgo y no contempló los modelos y sistemas de IA que pueden aplicarse a usos muy diversos y por tanto implicar -o no-, un riesgo elevado según las circunstancias.

En particular, los llamados *modelos* son esenciales para el funcionamiento de sistemas de IA, incluso de sistemas de IA de capacidades generales, que se basan en ellos.[62] La necesidad de abordar de algún modo tanto esos modelos como los sistemas de muy amplio espectro se hizo especialmente patente tras la irrupción de las herramientas de inteligencia artificial generativa como ChatGPT, aunque ya se había sugerido su incorporación al Reglamento con anterioridad.[63] La versión final del Reglamento acoge estas figuras, con la denominación de *modelos de IA de uso general* y de *sistemas de IA de uso general*. No se acoge, pues, la denominación de "modelo fundacional",[64] que había sido sugerida por el Parlamento en sus enmiendas.

Un *modelo de IA de uso general* se define como «un modelo de IA, también uno entrenado con un gran volumen de datos utilizando la autosupervisión a gran escala, *que presenta un grado considerable de generalidad* y es *capaz de realizar de manera competente una gran variedad de tareas distintas*, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede inte-

---

[62] Entre otros muchos ejemplos, Gemini (Google), GPT-4 (OpenAI), o Claude (Anthropic), se suelen considerar modelos de uso general, a partir de los cuales funcionan sistemas de IA.

[63] Véase, por ejemplo: Future of Life Institute: *General Purpose AI and the AI Act*, May 2022, disponible en https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf. Otras propuestas posteriores pueden verse en HELBERGER, N; DIAKOPOULOS, N.: «ChatGPT and the AI Act», *Internet Policy Review*, 12(1), 2023, https://doi.org/10.14763/2023.1.1682.

[64] Ha popularizado esta denominación el Center for Research on Foundation Models (CRFM), del Stanford Institute for Human-Centered Artificial Intelligence (HAI), dedicado al estudio de estos modelos, sobre los que ha publicado diversos estudios (https://crfm.stanford.edu/).

grarse en diversos sistemas o aplicaciones posteriores».[65] En cambio, un *sistema de IA de uso general* es «un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA».[66]

Como explican los considerandos, los modelos son componentes esenciales de los sistemas de IA, en los que están integrados y de los que forman parte, pero no constituyen por sí mismos un sistema de IA, pues para ello sería preciso añadirles otros componentes, como una interfaz de usuario. Por otra parte, los modelos de IA de uso general pueden introducirse en el mercado a través de APIs (*Application Programming Interface*), o mediante bibliotecas (*libraries*), ya sea como descarga directa o como copia tangible.[67]

Pues bien, dentro de los modelos de IA de uso general, se distinguen, como una subcategoría, aquellos que presentan *riesgos sistémicos*, esto es, «un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor».[68] Estos riesgos, que son más elevados cuanto mayores sean las capacidades de los modelos, pueden surgir durante todo el ciclo de vida del modelo y están afectados por múltiples factores.

En particular, se considerará que un modelo de uso general presenta un riesgo sistémico a partir de cierto umbral de cantidad acumulada de cálculos utilizada para su entrenamiento, medida en operaciones de coma flotante, umbral que la Comisión podrá modificar para reflejar el estado actual de la técnica.[69] Los modelos de IA de uso general de riesgo sistémico se hallan sujetos a obligaciones más rigurosas de control, evaluación, documentación, vigilancia y ciberseguridad.

---

[65] Art. 3.63 RIA (énfasis añadido). A fin de excluirlos de la correspondiente regulación, se exceptúan de la definición «los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización».

[66] Art. 3.66 RIA.

[67] Cfr. cdo. 97 RIA.

[68] Art. 3.65) RIA.

[69] Art. 51 RIA.

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 sinfín 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 werables 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 amplías 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.

9 788410 707085