

**LA RESPONSABILIDAD CIVIL
DERIVADA DE LOS DAÑOS CAUSADOS
POR SISTEMAS INTELIGENTES
Y SU ASEGURAMIENTO**

**Análisis del tratamiento ofrecido
por la Unión Europea**

Manuel ORTIZ FERNÁNDEZ



Dykinson, S.L.

**LA RESPONSABILIDAD CIVIL DERIVADA
DE LOS DAÑOS CAUSADOS
POR SISTEMAS INTELIGENTES
Y SU ASEGURAMIENTO**

Análisis del tratamiento ofrecido por la Unión Europea

**LA RESPONSABILIDAD CIVIL
DERIVADA DE LOS DAÑOS CAUSADOS
POR SISTEMAS INTELIGENTES
Y SU ASEGURAMIENTO**
Análisis del tratamiento ofrecido
por la Unión Europea

Manuel Ortiz Fernández

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).

Dirijase 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

© Copyright by
Manuel Ortiz Fernández
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: 978-84-1377-781-8
Depósito Legal: M-27507-2021

ISBN electrónico: 978-84-1377-843-3

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

Índice

I. CONSIDERACIONES PRELIMINARES.....	9
II. LA DENOMINADA INTELIGENCIA ARTIFICIAL: ENTRE EL MITO Y LA REALIDAD	23
1. CONCEPTO DE INTELIGENCIA ARTIFICIAL Y CARACTERÍSTICAS BÁSICAS	24
2. BREVE REFERENCIA AL FUNCIONAMIENTO DE ESTA TECNOLOGÍA.....	29
3. RECAPITULACIÓN: ¿EXISTEN REALMENTE LA INTELIGENCIA ARTIFICIAL Y LA AUTONOMÍA EN LA ACTUALIDAD?	34

III. LA SEGURIDAD Y LA ÉTICA APLICABLES EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL: la propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (<i>artificial intelligence act</i>).....	39
IV. EL TRATAMIENTO OFRECIDO POR LAS INSTITUCIONES EUROPEAS A LA RESPONSABILIDAD CIVIL: especial atención a la Resolución del Parlamento Europeo, de 20 de octubre de 2020 y a la propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial	53
1. CONSIDERACIONES GENERALES.....	53
2. LA POSIBLE APLICACIÓN DE LA DIRECTIVA 85/374, DE 25 DE JULIO DE 1985 Y LAS ADAPTACIONES NECESARIAS	60
3. LA PROPUESTA DE REGLAMENTO SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL.....	72
3.1. Ámbito subjetivo de aplicación: la figura del «operador»	72
3.2. La necesidad de concretar un ámbito material de aplicación	81
3.3. La clasificación de los sistemas de inteligencia artificial.....	83

- 3.4. Los criterios de responsabilidad incluidos en la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial..... 103

V. EL ASEGURAMIENTO DE LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL..... 121

1. CONCEPTUALIZACIÓN GENERAL DE LOS SEGUROS DE RESPONSABILIDAD CIVIL: EL RIESGO COMO CRITERIO PARA EXIGIR SU OBLIGATORIEDAD..... 123
2. EL ASEGURAMIENTO OBLIGATORIO EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL Y SU COBERTURA .. 125
3. EL CIBERSEGURO COMO POSIBLE MODALIDAD PARA LA INTELIGENCIA ARTIFICIAL Y SUS CARENCIAS: LA NECESIDAD DE CREAR UN SEGURO ESPECÍFICO.... 132
4. LA RELEVANCIA DE DISPONER DE UN REGISTRO Y DE ESTABLECER FONDOS DE COMPENSACIÓN 137

VI. REFERENCIAS BIBLIOGRÁFICAS 141

I.

CONSIDERACIONES PRELIMINARES

La irrupción de las nuevas tecnologías y, en concreto, de la denominada inteligencia artificial es un hecho contrastable¹. A nadie se escapa que, en la actualidad, la implementación de sistemas que incorporan estas redes neuronales ha aumentado exponencialmente. Este desarrollo se debe a la búsqueda de máquinas inteligentes y autónomas que puedan llevar a cabo tareas que, en principio, estaban reservadas a los seres humanos. De algún modo, con ello se pretende mejorar y optimizar los resultados, así como reducir el coste de tiempo empleado. A este respecto, es indudable que se han conseguido grandes logros y beneficios. Así, no se puede obviar que existen diferentes sectores en los que se ha incorporado (o se incorporará en un periodo de tiempo reducido) la inteligencia como, por ejemplo, el sector de los vehículos autónomos, de los drones, de los robots asistenciales o sanitarios² o sistemas de clasificación de bases de datos.

¹ En este sentido, GARCÍA TERUEL, R.M.: «El derecho de daños ante la inteligencia artificial y el *machine learning*: una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea», en *Cuestiones clásicas y actuales del Derecho de Daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón* (Coord. J. ATAZ LÓPEZ/J.A. COBACHO GÓMEZ), Navarra, Aranzadi, 2021, p. 1013 incluso alude a que estamos ante disciplina en sí misma, debido a su impacto y al especial interés en que se desarrolle.

² Sobre el particular, *vid.* NAVAS NAVARRO, S.: «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)*, Granada, Comares, 2021,

No obstante, esta nueva realidad no evita que existan voces contrarias a dicha tecnología y que sea preciso realizar un análisis exhaustivo acerca de las implicaciones que conllevan. Desde nuestra perspectiva, a pesar de que los resultados obtenidos son muy positivos, entendemos que las ciencias sociales han de ocupar un papel esencial para evitar que se produzcan situaciones poco deseables³. Los avances tecnológicos, tan necesarios, han de ir acompañados de una ética adecuada⁴ y han de respetar, en últi-

pp. 1-50. Asimismo, lo cierto es que en el ámbito de la inteligencia artificial pueden surgir diversas particularidades relacionadas con el consentimiento informado como, por ejemplo, la necesidad de que se incorpore información específica sobre la tecnología que se va a emplear e, incluso, el modo en que, en su caso, ha de prestar dicha información una máquina inteligente. A este respecto, *vid.* COHEN, I.G.: «Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?», *Georgetown Law Journal*, vol. 108, 2020, pp.1425-1469; EVANS, B.J./PASQUALE, F.: «Product Liability Suits dor FDA-Regulated AI/ML Software», *SSRN*, 2020, pp. 1-15.

³ En este sentido, JAUME-PALASÍ, L.: «Cómo la inteligencia artificial está impactando en las sociedades», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, p. 28 pone de relieve que «La IA –los sistemas algorítmicos– abarca tecnologías cuya esencia, impacto y riesgos siguen siendo objeto de escrutinización y disputa científica. La IA y los sistemas algorítmicos no entienden al individuo. Conceptualmente, representan ideas de lo social. La forma en que calculan y clasifican patrones es relacional. Los algoritmos clasifican a las personas en grupos granulares. La identidad de los individuos no es relevante. Si bien la personalización puede ser percibida por el usuario como un procedimiento técnico de individualización, técnicamente, la personalización no implica individualización alguna. Es un procedimiento relacional: la personalización meramente clasifica al individuo en colectivos muy específicos de personas con similitudes».

⁴ A este respecto, destaca KEMP, R.: «Artificial Intelligence: introduction», *Practical Law UK Articles*, 2017, p. 2 que la cuarta revolución industrial en general y la inteligencia artificial en particular plantean profundas preguntas sobre la naturaleza, el momento y el alcance del surgimiento de nuevas industrias, el desplazamiento del empleo, el cambio social y la ética. En este sentido, la inteligencia artificial es una de las áreas de innovación digital que se están desarrollando cada vez más rápidamente e interactuando entre sí de formas cuyas consecuencias son difíciles de prever. Un acrónimo útil para estos cambios es la “cuarta revolución industrial”.

ma instancia, los derechos subjetivos de los particulares. Además, la introducción de muchas de estas cuestiones exige que se produzca un cambio de paradigma⁵, esto es, es preciso que se lleve a cabo una reflexión profunda en los ámbitos cultural, ético, jurídico y político en los distintos estados. No debemos olvidar que los presupuestos y esquemas que se manejan quedarán desplazados con las modernas tecnologías y ello obliga a que nos replanteemos ciertas premisas.

En este marco, debemos, pues, afrontar las diversas problemáticas derivadas del uso de la inteligencia artificial tratando de ofrecer la respuesta que se presente como más correcta por acoger al mayor número de intereses en juego. En este sentido, el desarrollo y la implementación de la inteligencia artificial en diversos sectores⁶ provoca que nos preguntemos si estos riesgos

⁵ Al aproximarnos a cualquier ámbito de la realidad, en general y, del Derecho, en particular, hemos de evitar adoptar posicionamientos radicales. Así, suele ser habitual encontrar dos tipos de planteamientos a la hora de interpretar un hecho que, en mayor o medida, implique una modificación de los esquemas que veníamos manejando. De un lado, se ubican aquellos que siempre entienden que no estamos ante un verdadero cambio y que contamos con suficientes criterios para resolver las problemáticas que se puedan plantear. Este colectivo se caracteriza, pues, por recurrir a herramientas tradicionales y mostrarse reacios y reaccionarios a los nuevos escenarios. De otro lado, aquellos que, siempre y en todo caso, consideran que es preciso adoptar nuevas normas y valores porque se trata de una alteración sustancial. Desde nuestra perspectiva, lo más correcto es incorporar una postura intermedia que valore *ad casum* y que, reconociendo las particularidades del contexto que se presenta, tenga en cuenta la tradición jurídica, el ordenamiento jurídico y los mecanismos de que disponemos. Pues bien, ello es especialmente importante en el ámbito de la inteligencia artificial, donde ha de imponerse la lógica y el sentido común, tan denostados en ocasiones. Y esto último pasa por no obviar que nos movemos ante un sector moderno y, en cierta medida, desconocido sobre el que debemos aplicar tanto medidas “tradicionales” como novedosas.

⁶ Para visualizar un estudio sobre el estado de la inteligencia artificial y las tendencias de investigación en este campo, *vid.* “Artificial Intelligence and Life in 2030”, One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, September 2016, realizado

estarían cubiertos por un eventual seguro de responsabilidad o si, por el contrario, requieren de la suscripción de una modalidad especial. Asimismo, es particularmente complicado concluir quién es el sujeto responsable, lo que dificulta, más si cabe, la tarea anterior. Igualmente, debemos reflexionar sobre otras problemáticas íntimamente ligadas, a saber, los criterios de imputación, el recurso a posibles teorías que suavicen el *onus probandi*, la causalidad, etc. De esta forma, pese al ámbito de aplicación de la Directiva sobre responsabilidad por productos defectuosos, el marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, ya que un robot podría aprender de forma autónoma de sus experiencias concretas e interactuar con su entorno de un modo imprevisible y propio.

Para presentar una respuesta a estas cuestiones⁷, se hace necesario analizar los documentos y resoluciones emitidas por las

por AI100 Group. El citado estudio se encuentra disponible en: https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf (fecha última consulta 03.01.2021). Así, por ejemplo, en el ámbito jurídico, señala HOLME, D.: «Using artificial intelligence: not pie in the sky», *Practical Law UK Articles*, 2017, p. 2 que, si bien IBM Watson podría ser el ejemplo más famoso de uso de inteligencia artificial en el sector legal, se han lanzado varias otras aplicaciones basadas en el procesamiento del lenguaje natural, el aprendizaje automático y otras técnicas de inteligencia artificial para abordar las diferentes etapas de un contrato. Igualmente, sobre el impacto de la inteligencia artificial en la toma de decisiones arbitrales, *vid.* NAPPERT, S.: «The challenge of artificial intelligence in arbitral decision-making», *Practical Law UK Articles*, 2018, pp. 1-7.

⁷ Para un estudio pormenorizado de las mismas, *vid.* LACRUZ MANTECÓN, M.L.: «Cibernética y Derecho europeo: ¿una inteligencia robótica?», *Diario La Ley*, núm. 9376, 2019, pp. 1-19; *Robots y personas. Una aproximación jurídica a la subjetividad cibernética*, Madrid, Reus, 2020; ZURITA MARTÍN, I.M.: *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Madrid, Reus, 2020; BARRIO ANDRÉS, M.: *Manual de Derecho Digital*, Valencia, Tirant lo Blanch, 2020.

instituciones europeas⁸ y sus organismos de apoyo, con el fin de buscar criterios que nos permitan dilucidar las particularidades aplicables a este campo⁹. Así, trataremos de extraer los principios¹⁰, reglas o valores establecidos por la Unión Europea en esta materia. No tenemos que perder de vista que, al margen de las disposiciones nacionales generales sobre responsabilidad civil, los estados miembros no cuentan con una normativa específica al respecto¹¹, por lo que es importante que procedamos a exami-

⁸ En este sentido, la preocupación de la Unión Europea por estas materias se puede observar en el Programa específico FP7-SIS, «capacidades: ciencia y sociedad», 2006/974/EC, de 19 de diciembre de 2006, donde se enmarcó el proyecto «robolaw» sobre la «regulación de las tecnologías robóticas emergentes en Europa. La robótica frente al derecho y la ética».

⁹ Sea como fuere, como ponen de relieve ČERKA, P./GRIGIENĖ, J./SIRBIKYTĖ, G.: «Liability for damages caused by artificial intelligence», *Computer Law & Security Review*, vol. 31, núm. 3, 2015, p. 377, el problema de la regulación legal de la inteligencia artificial no solamente debe resolverse en Europa y no puede limitarse por la territorialidad y las prácticas de diferentes tradiciones legales. En este sentido, esta problemática se extiende más allá de las fronteras nacionales al ser de importancia mundial.

¹⁰ Sobre este particular, *vid.* TAPIA HERMIDA, A.J.: «Decálogo de la inteligencia artificial ética y responsable en la Unión Europea», *Diario La Ley*, núm. 9749, sección Tribuna, 2020, pp. 1-7.

¹¹ En este sentido, únicamente países como China, Japón, Corea del Sur o Estados Unidos cuentan con cierta regulación al respecto. A este respecto, cabe destacar la labor realizada por los comités especializados en Estados Unidos (el *Committee on Science* y el *Committee on Technology*) que se enmarcan en el *National Science and Technology Council Committee on Technology* (NSTC). Igualmente, en Reino Unido, debemos reseñar el Comité de Ciencia y Tecnología de la *House of Commons*, que publicó un informe sobre robótica e inteligencia artificial recomendando el establecimiento de una Comisión Permanente de Inteligencia Artificial y un Consejo de Liderazgo en Robótica y Sistemas Autónomos. En dicho informe, no obstante, se alertaba de la importancia de la rendición de cuentas para las armas autónomas, ya que es patente la tendencia hacia una mayor autonomía en los sistemas militares. *Vid.* STC: Robotics and artificial intelligence (12 October 2016), disponible en: <https://publications.parliament.uk/pa/cm201617/cmselect/cmstech/145/145.pdf> (fecha última consulta: 03.01.2021).

nar dichos textos. En especial, tanto por su actualidad como por la relevancia de su contenido, cobra relevancia la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial¹². En este sentido, se incorpora una Propuesta de Reglamento que, en un futuro, de ser aprobada, será la norma de referencia en este campo. No obstante, como veremos, en esta última disposición se recogen una serie de principios que pueden entrar en conflicto.

Asimismo, cabe reseñar la Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) y que modifica determinadas normas de la Unión¹³, que será analizada más tarde.

De hecho, con el citado estudio se podrá comprobar tanto la relevancia de la temática escogida (como lo demuestra el gran número de pronunciamientos de la Unión Europea¹⁴) como las

¹² (2020/2014(INL), P9_TA-PROV(2020)0276, Régimen de responsabilidad civil en materia de inteligencia artificial.

¹³ COM/2021/206 final, disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (fecha de última consulta: 25.05.2021).

Asimismo, sus anexos se encuentran disponibles en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF (fecha de última consulta: 25.05.2021).

¹⁴ A este respecto, a las ya mencionadas debemos de anudar, entre otras, la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Inteligencia Artificial para Europa, de 25 de abril de 2018 y su documento de acompañamiento; la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, En ruta hacia la movilidad automatizada: estrategia de la UE para la movilidad del futuro, de 15 de mayo de 2018; el Informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies»; el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité

variaciones que ha recibido el tratamiento ofrecido al respecto. Entre otras cuestiones, cabe destacar la atribución de personalidad jurídica a estos sistemas, el tipo de responsabilidad que se ha de aplicar, la exigencia de un seguro obligatorio o la constitución de los denominados fondos de compensación. En esta línea, a pesar de que las instituciones europeas se mostraron favorables a determinadas ideas en sus primeras manifestaciones (*vid.* Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica¹⁵), lo cierto es que ha rechazado o matizado algunas de ellas en documentos posteriores (*vid.*, por ejemplo, la precitada Resolución del Parlamento Europeo, de 20 de octubre de 2020).

Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020 que acompaña al Libro Blanco sobre la inteligencia artificial; la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, (2020/2012(INL), P9_TA-PROV(2020)0275); la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial (2020/2015(INI), P9_TA(2020)0277).

¹⁵ (2015/2103(INL)). Normas de Derecho civil sobre robótica, P8 TA(2017)0051. A ello hay que sumar el Informe de la Comisión de Asuntos Jurídicos con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)). Este informe, además de recoger la citada resolución, incorpora la opinión de las diversas comisiones competentes. En este sentido, señala la Comisión de Asuntos Jurídicos que «El comportamiento de un robot podría tener implicaciones de Derecho civil, tanto en términos de responsabilidad contractual como extracontractual. Por lo tanto, es necesario aclarar la responsabilidad de las acciones de los robots y, en última instancia, la capacidad jurídica o el estatus de los robots y de la inteligencia artificial, con el fin de garantizar la transparencia y la seguridad jurídica para los productores y consumidores en la Unión Europea».

En todo caso, a nuestro entender, tal investigación ha de estar basada en una serie de premisas que traten de asegurar, en última instancia, dos extremos que, en ocasiones, pueden encontrarse enfrentados. De un lado, se ha de tratar que los daños causados reciban una adecuada cobertura, esto es, que las víctimas obtengan un resarcimiento proporcionado, sin que quepa excluir la responsabilidad por el mero hecho de que el perjuicio se haya producido por una máquina inteligente. Entre otras, se pretende amparar este objetivo con algunas medidas como el aseguramiento obligatorio (de algunos sistemas), con el establecimiento de un fondo de compensación, con la necesaria intervención de un ser humano en todas las actividades que lleve a cabo el robot, con un concepto amplio de daño indemnizable o con unos criterios de imputación severos.

De otro lado, consideramos que la propuesta por la que se opte ha de evitar que, en la medida de lo posible, se reduzca la inversión en este sector, ya que repercutiría en la propia mejora y detrimento de la calidad de vida de las sociedades contemporáneas (y futuras). En este sentido, se ha de promocionar y favorecer el desarrollo de la innovación y de las tecnologías, que se consideran fundamentales. No se puede obviar que estas últimas ocupan un papel esencial y esta tendencia aumentará con el paso del tiempo. Para ello, una de las cuestiones primordiales es proporcionar seguridad jurídica a todas las partes intervinientes. En este campo, uno de los obstáculos que debe salvarse es la inflación regulatoria¹⁶ y la excesiva burocratización. Íntimamente liga-

¹⁶ A este respecto, se alude al «principio de neutralidad tecnológica» cuyo concepto es, no obstante, discutido. Al margen de ello, lo cierto es que se ha incluido en diferentes normas europeas y podemos señalar que su finalidad última del mismo es asegurar que las autoridades adopten un papel «neutral» a la hora de establecer la tecnología que se ha de emplear. En este sentido, CULLELL MARCH, C.: «El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico», *IDP. Revista de Internet, Derecho y Política*, núm. 11, 2010, p. 2 destaca que «ante las diferentes opciones tecnológicas y de servicios que brindan las nuevas tecnologías, las autoridades de regulación adop-

do a lo anterior, se prevé como finalidad última, la armonización de la legislación en el Mercado Único Digital. Precisamente en esta línea se manifiesta la precitada Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) y que modifica determinadas normas de la Unión.

Sin duda, estas reglas pueden entrar en colisión, siendo necesario realizar una adecuada ponderación de intereses y determinar un equilibrio difícil de alcanzar. A nadie escapa que, si para tutelar los derechos de los afectados se aumentan los requisitos y se imponen unas pautas objetivas de responsabilidad, ello podrá derivar en un descenso de la inversión en este sector y, por tanto, en un menor progreso tecnológico.

Por todo ello, en primer lugar, desde nuestra perspectiva, el criterio fundamental que debe operar en este sector es el riesgo, esto es, el peligro potencial que se genera como consecuencia de implementar este tipo de tecnología. A este respecto, el mismo ha de ser tenido en cuenta a la hora de efectuar la clasificación entre los sistemas de inteligencia artificial que, a su vez, tal y como veremos, repercute en el propio tipo de responsabilidad que se aplica y la exigencia de aseguramiento. En segundo lugar, el grado de automatización y, por tanto, el nivel de autonomía de las máquinas inteligentes es relevante para atribuir personalidad jurídica a dichos sistemas y, por ende, responsabilidad civil. Como se puede comprobar, ambos se encuentran referidos a realidades que, si bien se encuentran ligadas, no pueden confundirse.

tarán un papel neutral con relación a la tecnología a emplear y los servicios a prestar –principio de neutralidad tecnológica y de servicios–, superando así el modelo rígido y centralizado que ha caracterizado la regulación del espectro hasta el momento. La disminución de la presión reguladora es una característica de las nuevas formas de gestión que promueven la creación de un mercado del espectro a nivel regional y nacional».

Relacionado con lo anterior, muy resumidamente, los tres problemas o desafíos a los que se enfrenta la inteligencia artificial pueden resumirse en los siguientes. Por un lado, la idea de que la intervención del ser humano es siempre necesaria (en todos los momentos) se encuentra muy arraigada en la sociedad actual. De hecho, la propia política de la Unión Europea ha acogido la misma y apuesta por un grado de automatización más reducido y en el que exista una supervisión por parte de una persona. Sin embargo, tal y como señalaremos, consideramos que este extremo no es totalmente correcto y que puede disminuir la financiación de este sector o, al menos, influir en la política de las compañías (como se puede comprobar, por ejemplo, en el campo del transporte y la apuesta realizada por Tesla en sus vehículos). Precisamente, por este motivo indicábamos anteriormente que la autonomía no ha de tenerse en cuenta a la hora de valorar los sectores de alto riesgo.

De alguna forma, se encuentra implantada la convicción de que, cuando mayor es esta (y menor, por tanto, el control humano), la probabilidad de que se produzca un daño es también más elevada. Desde nuestra perspectiva, esta premisa aceptada *per se et iure et de iure* nos parece, cuanto menos, aventurada y sin base científica. Así, no solamente consideramos que no es adecuado suponer tal extremo, sino que podemos presumir (*iuris tantum*) que la tecnología eliminará gran parte de los riesgos de la actividad en la que se incorpore. De hecho, una de las principales problemáticas frente a las que se ha de reaccionar es el peligro de que, al crear los sistemas, los humanos trasladen sus sesgos o prejuicios, por lo que no se puede concluir que la intervención humana disminuya o elimine el riesgo.

Por otro lado, íntimamente relacionado con lo destacado, se suele entender que la tecnología va a sustituir a los humanos en sus empleos y, por tanto, va a repercutir en el ámbito laboral. Sin negar lo cierto de esta cuestión, entendemos que ello no ha de suponer un obstáculo para el desarrollo y que se han de buscar fórmulas

para tratar de salvar este problema. Por último, se alude al peligro de que una máquina interactúe con las personas en los supuestos en los que un error de estas pueda conllevar también un fallo de la primera¹⁷. Sin embargo, no estamos ante un verdadero inconveniente o, al menos, no es insalvable. Máxime porque cuando una actividad concreta esté formada, en su totalidad, por robots inteligentes, no se producirán estas disquisiciones. En este sentido, como destacamos anteriormente, el aprendizaje de los sistemas reducirá considerablemente estas situaciones conflictivas al minimizar la probabilidad de que se produzca un evento dañoso. En definitiva, el temor –en muchas ocasiones, infundado– o la cultura de una determinada época no debería actuar en contra de la evolución de la tecnología y, en suma, de un aspecto tan esencial como es la innovación. Más tarde volveremos sobre estos asuntos.

En otro orden de cosas, no hay que perder de vista que la responsabilidad civil tiene un campo concreto de actuación y que el mismo cobra vigencia *ex post*, esto es, una vez producido el hecho dañoso. No obstante, existen otros sectores del Derecho privado, así como otras ramas del ordenamiento jurídico u otras disciplinas que pueden ofrecer mecanismos muy relevantes y que, en algunos casos, permiten actuar de forma apriorística para prevenir o reducir el perjuicio¹⁸. De hecho, estos últimos adquieren, incluso, mayor relevancia y se presentan como una solución más eficaz. Desde esta perspectiva, lo ideal es que el Derecho de Daños únicamente intervenga de forma (casi) excepcional, en aquellos supuestos en los que las herramientas que despliegan sus efectos *ex ante* no hayan podido alcanzar su finalidad.

Por este motivo, dedicaremos una parte del presente estudio a analizar, siquiera brevemente, el papel que deben desempeñar

¹⁷ Para más información, *vid.* SELBST, A.D.: «Negligence and AI's Human Users», *Boston University Law Review*, vol. 100, 2020, pp. 1315-1376.

¹⁸ En este sentido, *vid.* RUBÍ PUIG, A.: «Retos de la inteligencia artificial y adaptabilidad del derecho de daños», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, p. 59.

tanto la ética como las normas de seguridad en este campo. Sin duda, estas últimas pueden resultar fundamentales para que se establezcan unos parámetros que redunden en una inteligencia artificial fiable y que genere confianza.

En definitiva, hemos de tener en cuenta que nos encontramos ante una materia compleja, en la que inciden, transversalmente, diversas realidades. Ofrecer, pues, una solución única, se presenta como una tarea casi inalcanzable, como lo demuestra la ingente cantidad de documentos emitidos desde instancias europeas. No obstante, podemos tratar de establecer unas premisas básicas¹⁹ que consideramos fundamentales para que se produzca un adecuado tratamiento de la cuestión²⁰ y se resarza, en definitiva, el posible perjuicio producido. Por este motivo, un estudio completo (que escapa a la finalidad de esta obra) exigiría analizar las implicaciones de cada uno de ellos y sus características particulares. Adquieren vigencia, por tanto, todas las ramas del Derecho

¹⁹ En este sentido, FERREIRA, A.E.: «Partilhar o mundo com robôs autónomos: a responsabilidade civil extracontratual por danos. introdução ao problema», *Cuestiones de Interés Jurídico*, IDIBE, 2017, p. 25 destaca que «En el futuro, en las relaciones de responsabilidad entre seres humanos y robots, se podrá trabajar en determinados institutos jurídicos para adaptar las soluciones, a saber: a) el requisito del consentimiento informado para ser tratado por un robot; (b) una redefinición de la responsabilidad del productor por el suministro de actualizaciones y sus derechos de presentación de informes; (c) una obligación clara para quienes se benefician del trabajo de robots autónomos; (d) la existencia de fondos de seguros/garantías relativos al uso de robots. No le pide a la economía de este artículo abordar cada una de estas cuestiones, pero creemos que se trata de vértices fundamentales en la construcción de un modelo doctrinal suficientemente actualizado y completo».

²⁰ Para más información, *vid.* MONTERROSO CASADO, E.: «Repercusiones de la inteligencia artificial en el ámbito de la responsabilidad civil», *Revista de responsabilidad civil, circulación y seguro*, núm. 11, 2010, pp. 6-20; RAMÓN FERNÁNDEZ, F.: «Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?», *Diario La Ley*, núm. 9365, 2019; NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Madrid, Reus, 2019.

(público y privado), ya que se ven afectados distintos ámbitos del mismo. Así, se hace necesario tutelar los derechos fundamentales (como la intimidad o la integridad física y moral), la protección de datos y de los consumidores y usuarios, la propiedad intelectual e industrial, entre otros. Sea como fuere, el objetivo pretendido con este análisis es mucho menos ambicioso. En este sentido, únicamente pretendemos esclarecer, en cierta medida, el objeto de debate (cuestionando ciertas creencias establecidas) y focalizar los esfuerzos en el problema real que subyace a estas tecnologías.

II.

LA DENOMINADA INTELIGENCIA ARTIFICIAL: ENTRE EL MITO Y LA REALIDAD

A la hora de aproximarnos a un determinado ámbito, una de las cuestiones más importantes es la relativa a la corrección terminológica. Máxime cuando nos referimos a un sector específico y que pertenece a diversas disciplinas científicas (como ocurre con la inteligencia artificial). Sin embargo, esta tarea es excesivamente compleja para un lego en la materia y que no posee, por su formación, conocimientos suficientes para lograrlo. Por ello, a pesar de que trataremos de determinar aquellos conceptos más relevantes con el rigor que merecen, vaya por delante una disculpa del autor por las incorrecciones o imperfecciones que, de buen seguro, tendrán las líneas que se siguen²¹.

²¹ A este respecto, conviene tener en cuenta que en la presente investigación se emplearán indistintamente términos tales como sistemas de inteligencia artificial, máquinas inteligentes o robots autónomos. Somos conscientes, no obstante, de que, como tendremos ocasión de señalar, algunos no son totalmente correctos y de que, igualmente, no son conceptos totalmente equivalentes porque la aplicación de esta tecnología variará en función del ámbito en el que se implemente. A este respecto, ZURITA MARTÍN, I.: *La responsabilidad*, cit., p. 20.

No se puede obviar que, al menos inicialmente, la sensación es que nos estamos refiriendo a realidades que no existen en la actualidad y que, quizás, el nivel de desarrollo no llegue a ser tan elevado como para alcanzar este grado de innovación. No obstante, los esfuerzos se están centrando en avanzar en este sentido y, por tanto, hemos de tratar de determinar unas bases que nos permitan resolver los posibles conflictos que se produzcan en la práctica.

1. CONCEPTO DE INTELIGENCIA ARTIFICIAL Y CARACTERÍSTICAS BÁSICAS

A este respecto, conviene que, en primer lugar, establezcamos qué se viene entendiendo por sistema de inteligencia artificial²².

Por todo ello, quizás, el más adecuado es el de sistemas que incorporan tecnologías de *machine learning*, ya que parece englobar al resto. Sin embargo, para evitar reiteraciones innecesarias, por el propio uso generalizado de algunos y porque entendemos que no resta corrección científica, recurriremos a ellos sin distinción alguna. Entiéndase el lector, pues, puesto sobre aviso sobre esta cuestión.

²² Parte de la doctrina destaca que, en términos legales, la inteligencia artificial es una combinación de software y datos. El software (instrucciones para el procesador del ordenador) es la implementación en el código del algoritmo de inteligencia artificial (un conjunto de reglas para resolver un problema). Lo que distingue la inteligencia artificial del desarrollo de software tradicional es, en primer lugar, que las reglas del algoritmo y la implementación de software pueden ser dinámicas y cambiar a medida que la máquina aprende; y en segundo lugar, los conjuntos de datos muy grandes que procesa la IA (como lo que originalmente se llamó *big data*). Los datos son los datos de entrada (conjuntos de datos de entrenamiento, pruebas y operativos); que los datos procesados por el ordenador; y los datos de salida (incluidos los datos derivados de la salida). No obstante, no podemos obviar que nos encontramos ante un concepto complejo y, en cierta forma, ambiguo. A este respecto, destaca la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial incluida en el el Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, de 5 de octubre de 2020 (2020/2014(INL)) que muchos de

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 inteligente.

En este sentido, se podría predicar tal rasgo de la misma si un humano no era capaz de diferenciarla de otra persona²³. 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 simularla²⁴. En suma, se trataba de que estos robots usaran el lenguaje, formaran abstracciones y conceptos y resolvieran problemas reservados para los seres humanos.

Para la Comisión Europea²⁵, «El término “inteligencia artificial” (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos». Por su parte, el grupo de expertos

los sistemas de inteligencia artificial no son tan diferentes de otras tecnologías basadas en programas informáticos aún más complejos. Por ello, aboga por la utilización del término «toma de decisiones automatizada». En este sentido, *vid.* KEMP, R.: «Legal Aspects of Artificial Intelligence», 2018, p. 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 última consulta: 03.01.2021).

²³ TURING, A.: «Computing Machinery and Intelligence», *Mind*, vol. LIX, núm. 236, 1950, pp. 433-460.

²⁴ En este sentido, MCCARTHY, J., *et al.*: «A proposal for the dartmouth summer research project on artificial intelligence», 1955, pp. 1-13. Disponible en: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> (fecha última consulta: 03.01.2021).

²⁵ Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia Artificial para Europa, de 25 de abril de 2018 (COM/2018/237 final).

de alto nivel sobre inteligencia artificial²⁶ pone especial énfasis en la «racionalidad», que hace referencia «a la capacidad de elegir la mejor acción posible para alcanzar un objetivo determinado, dados determinados criterios que es necesario optimizar y teniendo en cuenta los recursos disponibles».

En otro orden de cosas, el artículo 3 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial (en adelante, Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial), incluida en la reciente Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial), indica que por «sistema de inteligencia artificial» hemos de entender «todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la actuación, con cierto grado de autonomía, para lograr objetivos específicos».

Además, señala que se considerará autónomo cuando el sistema funcione «interpretando determinados datos de entrada y utilizando un conjunto de instrucciones predeterminadas, sin limitarse a ellas, a pesar de que el comportamiento del sistema esté limitado y orientado a cumplir el objetivo que se le haya

²⁶ Una definición de la inteligencia artificial: principales capacidades y disciplinas científicas. Así, se destaca que la inteligencia artificial opera «percibiendo el entorno en el que se encuentra inmerso el sistema a través de sensores, recopilando e interpretando datos, razonando sobre lo que percibe o procesando la información derivada de esos datos, decidiendo cuál es la mejor acción que puede realizar y actuando en consecuencia mediante accionadores, pudiendo así modificar el entorno. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores».

asignado y otras decisiones pertinentes de diseño tomadas por su desarrollador».

Como destaca MURPHY²⁷, 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 observe²⁸.

Además, al aproximarnos a estas cuestiones, hemos de tener presente que la doctrina diferencia entre dos tipos de inteligencia artificial²⁹. De un lado, la «inteligencia artificial débil», que se ha aplicado «a aquellos sistemas que únicamente parecen, conductualmente, tener un pensamiento inteligente similar al humano (simulan tener inteligencia), pero que en realidad no pasan de ser sistemas muy especializados que aplican técnicas más o menos complejas a la resolución de problemas muy concretos, hallándose lejos de mostrar cualquier síntoma revelador de estados cognitivos». De otro lado, la «inteligencia artificial fuerte» se encuentra referida a la «capacidad de un sistema para emular ciertos procesos cognitivos o capacidades generales del pensamiento humano

²⁷ MURPHY, R.R.: *Introduction to AI Robotics*, Massachusetts, The MIT Press, 2019, pp. 3-4.

²⁸ En este sentido, *vid.* ZURITA MARTÍN, I.: *La responsabilidad*, *cit.*, p. 12; CHURNIN, S.: *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*, Madrid, Servicio de Publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, 2011, p. 21.

²⁹ A este respecto, *vid.* SOLAR CAYÓN, J.I.: *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Navarra, Aranzadi, 2019, pp. 23-25.

(...) pudiendo además mejorar continuamente su rendimiento a medida que realizan dichas operaciones y aprenden de su propia experiencia».

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 humanos³⁰.

Por otro lado, tal y como señala el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020³¹, que acompaña al Libro Blanco sobre la inteligencia artificial³², es necesario aludir a la conexión que existe entre la inteligencia artificial, el internet de las cosas³³ y la robótica, ya que «Combinan la conectividad, la autonomía y la dependencia de datos para llevar a cabo tareas con poco o ningún control o supervisión humanos». Estas tres realida-

³⁰ En este sentido, SOLAR CAYÓN, *La Inteligencia*, *cit.*, p. 25.

³¹ COM/2020/64 final, disponible en: <https://op.europa.eu/es/publication-detail/-/publication/4ce205b8-53d2-11ea-aece-01aa75ed71a1/language-es/format-PDF> (fecha última consulta: 03.01.2021).

³² COM/2020/65 final, disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf (fecha última consulta: 03.01.2021).

Para más información, *vid.* FOUNTOUKAKOS, K., *et al.*: «European Commission strategy for data and AI: shaping a digital future», *Practical Law UK Articles*, 2020, pp. 1-5.

³³ Una definición del internet de las cosas la encontramos en la Recomendación UIT-T Y.2060, que señala que se trata de una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en las tecnologías interoperables de la información y la comunicación existentes y en evolución. La citada Recomendación puede consultarse en: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060> (fecha última consulta: 03.01.2021).

des (a las que debemos anudar el *Big Data*) se encuentran íntimamente ligadas, ya que el avance en una de ellas precisa, inexorablemente, del desarrollo de las otras.

En todo caso, la reciente Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) y que modifica determinadas normas de la Unión propone una única definición de inteligencia artificial que, además, pueda adaptarse a los cambios que se sucedan en el futuro. En este sentido, el artículo 3.1 de la citada Propuesta destaca que por sistema de inteligencia artificial hemos de entender aquel software desarrollado con una o más de las técnicas y enfoques enumerados en el Anexo I y que puede, para un conjunto dado de objetivos definidos por el ser humano, generar resultados como contenido, predicciones, recomendaciones, o decisiones que influyen en los entornos con los que interactúan. En cuanto a los citados enfoques del Anexo I, se entienden incluidos:

- Los enfoques de aprendizaje automático, incluido el aprendizaje supervisado, no supervisado y por refuerzo, utilizando una amplia variedad de métodos, incluido el aprendizaje profundo.
- Los enfoques basados en la lógica y el conocimiento, incluida la representación del conocimiento, la programación inductiva (lógica), las bases de conocimiento, los motores de inferencia y deductivos, el razonamiento (simbólico) y los sistemas expertos.
- Aquellos enfoques estadísticos, estimación bayesiana, métodos de búsqueda y optimización.

2. BREVE REFERENCIA AL FUNCIONAMIENTO DE ESTA TECNOLOGÍA

Por todo lo anterior, debemos poner especial atención en términos tales como *software*, *hardware*, algoritmo y robótica. A este

respecto, 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, los que permiten solucionar un problema³⁴. 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 “robot³⁵”.

³⁴ A este respecto, destacan ČERKA, P./GRIGIENĖ, J./SIRBIKYTĖ, G.: «Liability for damages», *cit.*, p. 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).

³⁵ Sobre el particular, destaca ZURITA MARTÍN, I.: *La responsabilidad*, *cit.*, 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.: «¿Qué es un robot?», en *Derecho de los robots* (Dir. M. BARRIO ANDRÉS), Madrid, Wolters Kluwer, 2018, p. 35, 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

Una vez realizado lo anterior, debemos contextualizar la inteligencia artificial en este ámbito, para lo cual es necesario definir el concepto de red neuronal. Esta última aparece como un conjunto de neuronas artificiales conectadas entre sí que se transmiten señales e información, imitando, por tanto, el funcionamiento del cerebro humano. Se trata, en suma, de un modelo que permite encontrar la combinación de parámetros más adecuada para solucionar un problema concreto. A este ejercicio, se le conoce como “entrenamiento”, de tal forma que una red que ha sido sometida al mismo podrá emplearse posteriormente para llevar a cabo predicciones o clasificaciones.

Así, cobran importancia tanto el *machine learning* como el *deep learning*³⁶. A pesar de que son conceptos casi análogos, podemos tratar de establecer, someramente, las diferencias entre ambos. En cuanto al primero, cabe destacar que se trata de algoritmos matemáticos que permiten a las máquinas aprender (de igual forma a la que lo llevamos a cabo los humanos). Por su parte, el *deep learning* forma parte del aprendizaje automático, ya que es un algoritmo que imita la percepción de las personas inspirada en nuestro cerebro y la conexión entre neuronas. Este método suele incorporar las redes neuronales a las que hacíamos referencia anteriormente (*deep neural networks*). Por todo ello, a pesar de que los dos aspiran a obtener un aprendizaje similar al del cerebro, la principal distinción se basa en el tipo de algoritmos que emplean en uno u otro caso (como regla ge-

como una suerte de robots especialmente reducidos y los *softbots* como programas informáticos orientados a realizar tareas autónomas.

³⁶ Dentro del *machine learning* suele incluirse, también, el denominado *reinforcement learning* (o aprendizaje reforzado). A este respecto, se centra en la determinación de las acciones que ha de escoger un sistema para maximizar la noción de premio acumulado. En otro orden de cosas, en contraposición al *machine learning* aparece el *machine reasoning*. En suma, ambos aprenden y se entrenan con base en los datos que manejan, siendo la diferencia fundamental que este último permite, además, abordar nuevos problemas con un enfoque de razonamiento deductivo e inductivo.

neral, árboles de decisión en el primero y redes neuronales en el segundo).

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 incorpora redes neuronales y diversos enfoques y técnicas³⁷. 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 tripulada³⁸ (UAS). Asimismo, cuando el sistema ope-

³⁷ Estas dos nociones de inteligencia artificial se ponen de relieve en el citado informe del grupo de expertos «Una definición de la inteligencia artificial: principales capacidades y disciplinas científicas» cuando destaca que:

«Los sistemas de inteligencia artificial (IA) son sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores.

La IA es una disciplina científica que incluye varios enfoques y técnicas, como el aprendizaje automático (del que el aprendizaje profundo y el aprendizaje por refuerzo constituyen algunos ejemplos), el razonamiento automático (que incluye la planificación, programación, representación y razonamiento de conocimientos, búsqueda y optimización) y la robótica (que incluye el control, la percepción, sensores y accionadores así como la integración de todas las demás técnicas en sistemas ciberfísicos)».

³⁸ Para más información, *vid.* CASTELLS I MARQUÈS, M.: «Drones recreativos: normativa aplicable, responsabilidad civil y protección de datos», *Revista de Derecho Civil*, vol. VI, núm. 1, 2019, pp. 297-333; TORRUBIA CHALMETA, B.:

ra en Internet y tiene acceso al *Big Data*, se optimiza el rendimiento del mismo, ya que los datos representan un elemento esencial de la inteligencia artificial.

A este respecto, los rasgos más característicos de esta son la autonomía, la automatización, la racionalidad y el aprendizaje. Si bien es cierto que en el estado actual de la ciencia no encontramos robots que funcionen de un modo totalmente autónomo y sin supervisión alguna (nivel máximo de automatización), no cabe duda de que en un futuro próximo existirán. A modo de ejemplo, en el ámbito de los UAS, la EASA (*European Union Aviation Safety Agency*), en el *European Plan for Aviation Safety* (EPAS) 2020–2024³⁹, estima que el nivel máximo de automatización de los drones se alcanzará en 2028.

Por su parte, en el campo de los vehículos autónomos⁴⁰ la automatización se clasifica en seis niveles⁴¹, donde el grado cinco representa el más elevado y en el que no es necesaria la intervención de la persona (donde se encuentra trabajando actualmente Google). Todo ello, viene representado en los tres escenarios posibles⁴² de *driver centric* (*pure driving*), *network centric* (*collaborative driving*) y *vehicle centric* (*adaptative behaviors*).

«Aeronaves civiles no tripuladas. Contexto y regulación», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 255-267.

³⁹ En este sentido, *vid.* <https://www.easa.europa.eu/document-library/general-publications/european-plan-aviation-safety-2020-2024> (fecha última consulta: 03.01.2021).

⁴⁰ Para un estudio sobre la cuestión, *vid.* LACRUZ MANTECÓN, M.L.: «Inteligencia artificial y coches autónomos: análisis jurídicos europeos», *Revista Crítica de Derecho Inmobiliario*, núm. 775, 2019, pp. 2373-2409.

⁴¹ Así, los niveles de autonomía de los vehículos pueden resumirse en: nivel 0: sin asistencia; nivel 1: conducción asistida; nivel 2: autonomía parcial; nivel 3: autonomía condicional; nivel 4: alta autonomía; nivel 5: autonomía completa.

⁴² Para más información, *vid.* IBÁÑEZ-GUZMÁN J./LAUGIER C./YODER J.D./THRUN S.: «Autonomous Driving: Context and State-of-the-Art», en *Handbook of Intelligent Vehicles* (edit. A. ESKANDARIAN), Londres, Springer, 2012, pp. 1271-

3. RECAPITULACIÓN: ¿EXISTEN REALMENTE LA INTELIGENCIA ARTIFICIAL Y LA AUTONOMÍA EN LA ACTUALIDAD?

Si analizamos todo lo que hemos expuesto hasta el momento, podemos señalar que, en la actualidad, no existe una verdadera inteligencia artificial general⁴³ o no lo es en el sentido propio de la palabra. Muy al contrario, disponemos de sistemas que, a partir de la atribución de gran una cantidad de datos, son capaces que establecer relaciones y distribuciones entre los mismos. Por este motivo, en realidad, no actúan de forma racional o autónoma. Si se quiere, nos encontramos ante una apariencia de tales características, esto es, ante una máquina que, en cierta medida, lleva a cabo actos que recuerdan al razonamiento humano⁴⁴. En palabras de LACRUZ MANTECÓN⁴⁵, «Si tratamos a los robots como personas es porque al exhibir resultados que nosotros alcanzamos pensando, creemos que también ellos piensan, y que por lo tanto son, como nosotros, personas. Esto es un error, el robot no piensa, computa, su inteligencia no pasa de ser lo que se conoce como IA “débil”. Lo que ocurre es que los resultados de su actividad pasan

1310; ABRAHAM, K.S./RABIN, R.L.: «Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era», *Virginia Law Review*, vol. 105, 2019, pp. 127-171.

⁴³ A este respecto, destaca BODEN, M.A.: *Inteligencia artificial*, Madrid, Turner, 2017, pp. 84-145 que si bien la antes referida inteligencia artificial fuerte no tiene cabida en la actualidad, cabe la posibilidad de que las máquinas alcancen la denominada «singularidad». En este sentido, señala la autora citada que es posible que estas máquinas alcancen un nivel de inteligencia superior al de los seres humanos.

⁴⁴ Desde nuestra perspectiva, parece, al menos, pretencioso buscar formar una realidad basada en otra que, en realidad, no conocemos en profundidad. En este sentido, se pretende crear una suerte de red cerebral artificial sin tener suficientes datos acerca de cómo funciona el propio cerebro humano. Por este motivo, sin negar la posibilidad de que, en futuro, se produzca tal hecho, lo cierto es que, en la actualidad, debemos ser más cautelosos.

⁴⁵ *Robots y personas, cit.*, p. 98.

por pensamientos que fingen ser una comunicación intencional. Y cuando se finge bien, el resultado puede pasar por el original, pero no lo es».

Ello no quiere decir, sin embargo, que estemos ante un estado definitivo de la tecnología y que no pueda mejorar hasta alcanzar un nivel de tales características, sino que no nos encontramos ante este escenario en estos momentos. A este respecto, destaca GARCÍA TERUEL⁴⁶ que «los robots han pasado de ser máquinas que ejecutan órdenes preestablecidas, al servicio del ser humano y para delegarles tareas arduas (como las que desarrollan los robots industriales), a antes que pueden llegar a tomar decisiones por sí mismos y que están llamados a superar la inteligencia humana a partir de 2045».

Desde esta perspectiva, ciertas afirmaciones que se vierten acerca de la inteligencia artificial merecen ser repensadas. Así, se señala, por ejemplo, que la inteligencia artificial tendrá, cuanto menos, los mismos sesgos, prejuicios y errores que los seres humanos por cuanto son estos últimos los que intervienen en su formación. Desde nuestra perspectiva, esta aseveración ha de ser matizada. No es cierto que la inteligencia artificial, en general, vaya a presentar estas características. Muy al contrario, este hecho se producirá cuando nos encontremos ante la que se puede denominar inteligencia artificial débil, es decir, la tecnología que manejamos actualmente. Sin embargo, no será predicable de la inteligencia artificial a la que aspiramos, a aquella que, de forma total, sea capaz de aprender, razonar y decidir por sí misma. Si se observa con detenimiento, nos estamos refiriendo a un elemento de volición, de libertad (mínima), que permitirá que los robots escojan la opción que se presenta más adecuada sin que nadie pueda asegurar, *a priori*, cuál será dicha voluntad⁴⁷.

⁴⁶ «El derecho», *cit.*, p. 1011. En igual sentido, KURZWEIL, R.: *The singularity is near. When humans transcend biology*, New York, Penguin Group, 2005, p. 98.

⁴⁷ A este respecto, BADILLO ARIAS, J.A.: «Responsabilidad civil y aseguramiento obligatorio de los robots», en *Inteligencia artificial y riesgos cibernéticos*

Una vez establecida la anterior correspondencia, se plantea, entonces, determinar si esta tecnología incorpora algún elemento novedoso que nos permita justificar la existencia de un tratamiento diferenciado. A este respecto, no se puede negar que la creación de máquinas o de un *software* sofisticado no aparecen como elementos desconocidos para la sociedad. No obstante, la peculiaridad que se predica de los modernos sistemas es la falta de conocimiento para establecer el modo en que han operado en un sentido u otro. En otras palabras, generalmente, el ser humano ha podido conocer y explicar el funcionamiento interno de una máquina de forma más o menos clara y precisa.

Sin embargo, este hecho no siempre se puede predicar de los nuevos robots inteligentes, ya que ejecutan procesos que no siempre son sencillos de explorar. En definitiva, la implementación de estos últimos tiene, principalmente, dos funciones o finalidades. De un lado, reducir el coste y el tiempo para obtener un resultado concreto. De otro lado, revisar el comportamiento de las personas, detectar más fácilmente los errores y ofrecer la solución óptima.

En suma, esta inteligencia presenta las propuestas que son más beneficiosas o correctas, sin que, en realidad, podamos determinar cómo han llegado a tal conclusión ni el motivo por el que es el desenlace adecuado. Por tanto, el elemento peculiar es, sin duda, el desconocimiento y la ausencia de certezas acerca del funcionamiento real de estas máquinas. Pongamos un ejemplo para ilustrar esta idea. Imaginemos un sistema que se emplea para

cos. Responsabilidades y aseguramiento (Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, p. 41 apunta que, «por mucho que se avance en la robótica, el aprendizaje y las decisiones autónomas de los robots van a derivar siempre de su creación y programación, y no de una capacidad volitiva propia, que nunca van a tener». Por ello, a pesar de entender que en el futuro tendrán un tratamiento diferente, propone una asimilación al régimen previsto para los animales que, pudiendo actuar de forma independiente e impredecible, no responden de los daños causados.

predecir una determinada patología de los pacientes a la cual se le permite acceder a todas las historias clínicas, así como a otra información relevante. Llegado el caso, ante un usuario concreto, en atención a todo el entramado de datos al que tiene acceso, determina que el paciente X tiene una probabilidad del ochenta por ciento de padecer la enfermedad Y. Por su parte, el profesional de la medicina, al estudiar la historia clínica del mismo, sus antecedentes y sus síntomas, obtiene una solución diferente. Ante este escenario, lo cierto es que, sin saber el motivo, el sanitario que posee en su haber más de treinta años de ejercicio en el campo de la medicina está optando por un resultado incorrecto.

Pues bien, desde esta óptica debemos examinar los potenciales conflictos que se generan con la tecnología actual. Si se observa con detenimiento, todo se reduce a cálculos probabilísticos y al tratamiento de una ingente cantidad de información. Es precisamente este hecho el que permite que la máquina lleve a cabo tareas que se encuentran reservadas para los humanos, ya que correlaciona tal magnitud de datos y de posibilidades, que ninguna persona podría ejecutar esta acción. En esencia, debemos dilucidar si estas características son suficientes para justificar un tratamiento diferenciado y cómo debe canalizarse el mismo.

III.

LA SEGURIDAD Y LA ÉTICA APLICABLES EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL: la propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*)

Una de las problemáticas que más ha preocupado a la Unión Europea ha sido la relativa a la seguridad y a la ética aplicable a este ámbito⁴⁸. En suma, se trata de asegurar que la implementación de estas tecnologías se lleve a cabo de una forma adecuada, tratando

⁴⁸ Así, PEGUERA POCH, M.: «En búsqueda de un marco normativo para la Inteligencia Artificial», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, p. 44 destaca que «a pesar de que se han producido ya importantes avances en algunas de las manifestaciones de la IA, nos encontramos todavía en una fase incipiente de su desarrollo, y se estima que probablemente aún estamos a tiempo de encauzar su avance a fin de asegurar que redunde en beneficio de la sociedad y se puedan evitar algunos de los riesgos apuntados. No, ciertamente, para frenar su adopción, sino más bien al contrario, para promo-

de evitar, en última instancia, la producción de daños. En este sentido, ya en la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica⁴⁹ se afirmaba incluso que «la humanidad se encuentra a las puertas de una era en la que robots, bots, andróides y otras formas de inteligencia artificial cada vez más sofisticadas parecen dispuestas a desencadenar una nueva revolución industrial» y que, por tanto, «resulta de vital importancia que el legislador pondere las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación».

Como anteriormente destacamos, ello se traduce en la pugna de dos principios: de un lado, el avance y el desarrollo tecnológico y, de otro, el establecimiento de un marco que transmita confianza a todas las partes implicadas. En esta línea, el grupo de expertos emitió las Directrices éticas para la inteligencia artificial:

verla, pero en condiciones que permitan un verdadero progreso al servicio de las personas».

⁴⁹ Normas de Derecho civil sobre robótica, 2015/2103(INL), P8_TA(2017)0051, disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf (fecha última consulta: 03.01.2021). Esta norma incluye, además, una carta sobre robótica, un código de conducta ética para los ingenieros en robótica y un código deontológico para los comités de ética de la investigación.

A ello hay que sumar el Informe de la Comisión de Asuntos Jurídicos con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)). Este informe, además de recoger la citada resolución, incorpora la opinión de las diversas comisiones competentes. En este sentido, señala la Comisión de Asuntos Jurídicos que «El comportamiento de un robot podría tener implicaciones de Derecho civil, tanto en términos de responsabilidad contractual como extracontractual. Por lo tanto, es necesario aclarar la responsabilidad de las acciones de los robots y, en última instancia, la capacidad jurídica o el estatus de los robots y de la inteligencia artificial, con el fin de garantizar la transparencia y la seguridad jurídica para los productores y consumidores en la Unión Europea». El mismo se encuentra disponible en: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.pdf (fecha última consulta: 03.01.2021).

para una inteligencia artificial fiable (abril de 2019)⁵⁰. El objetivo de este documento es, tal y como proclama, «promover una inteligencia artificial fiable» y dicha fiabilidad se apoya «en tres componentes que deben satisfacerse a lo largo de todo el ciclo de vida del sistema: a) la IA debe ser lícita, es decir, cumplir todas las leyes y reglamentos aplicables; b) ha de ser ética, de modo que se garantice el respeto de los principios y valores éticos; y c) debe ser robusta, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA, incluso si las intenciones son buenas, pueden provocar daños accidentales».

No obstante, el propio grupo de expertos reconoció que, a pesar de que lo ideal es que todos ellos actúen en armonía y de manera simultánea, pueden surgir tensiones en la práctica, por lo que la sociedad deberá esforzarse por resolverlas. La solución pasa, pues, por reconocer varias premisas. Por un lado, se considera que la inteligencia artificial se presenta como una tecnología muy relevante por los innumerables beneficios que genera (y puede generar). Por otro lado, es cierto y posible que estos sistemas, sin embargo, causen ciertos perjuicios⁵¹. Debido a esto último se ha de actuar tanto de un modo preventivo como reactivo. En el primer caso, incorporando una serie de disposiciones que determinen un nivel mínimo de precaución y diligencia, que será exigido a los sujetos que utilicen la inteligencia artificial. En este punto, podría ser interesante crear unas normas de calidad a las que las empresas dedicadas a estas tareas deberían adherirse y, en última instancia, cumplir. En el segundo caso, de-

⁵⁰ Disponible en: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines> (fecha última consulta: 03.01.2021).

⁵¹ Así, por ejemplo, uno de los problemas que se está produciendo es el denominado *Deepfake*, esto es, un aprendizaje profundo y falso. Se trata, en suma, de una tecnología basada en la inteligencia artificial que permite superponer el rostro de una persona en el de otra y falsificar, así, sus gestos, para hacernos creer que están haciendo o diciendo algo que no ha pasado en realidad. Acerca de esta cuestión, vid. CONWAY, J./FRITH, G.: «The rise of the deepfake: looking into a dystopian future?», *Practical Law UK Articles*, 2020, pp. 1-14.

tallando un régimen que, a la postre, resulte satisfactorio para las víctimas, reparando los menoscabos producidos. A este respecto, la responsabilidad civil ocupa, sin duda, un papel esencial para lograr tal finalidad.

Por todo lo anterior, puede comprobarse cómo las realidades a las que hacíamos referencia (Derecho, ética y seguridad o robustez) se encuentran íntimamente ligadas pues, en definitiva, aluden a un mismo escenario. En este sentido, el citado texto se divide en tres capítulos o bloques. En primer lugar, se abordan los «fundamentos de una IA fiable», centrándose en el papel que han de desempeñar los derechos fundamentales y su relación con los principios éticos. Así, la comisión de expertos apuesta por «un enfoque de la ética en la IA basado en los derechos fundamentales consagrados en los Tratados de la UE, la Carta de los Derechos Fundamentales de la Unión Europea (la “Carta de la UE”) y la legislación internacional de derechos humanos». En concreto, destaca la relevancia del respeto de la dignidad humana, de la democracia, la justicia y el estado de Derecho, la libertad individual, la igualdad (no discriminación y solidaridad), así como de otros derechos de los ciudadanos.

Además, a ello debemos anudar los principios éticos en el contexto de los sistemas de inteligencia artificial que se encuentran arraigados en los derechos fundamentales a los que aludíamos. Se trata de «imperativos éticos que los profesionales de la IA deben esforzarse en todo momento por observar». Estos principios son el respeto de la autonomía humana⁵², de prevención

⁵² Este principio pretende que las personas que interactúen con un sistema de inteligencia artificial mantengan su autonomía plena y efectiva, sin que estos los subordinen, coaccionen, engañen, manipulen, condicionen o dirijan de forma injustificada. De esta forma, los citados sistemas «deberían diseñarse de forma que aumenten, complementen y potencien las aptitudes cognitivas, sociales y culturales de las personas». Asimismo, se insiste en la necesidad de que se garantice la supervisión y el control humanos sobre los procesos de trabajo de estas tecnologías.

del daño⁵³, de equidad⁵⁴ y de explicabilidad⁵⁵. Sin embargo, el propio documento recoge las posibles tensiones existentes entre ellos (como entre los principios de prevención del daño y de autonomía humana), para lo cual no existe una solución establecida. Por tanto, no cabe esperar que los profesionales encuentren la respuesta óptima basándose en los citados principios, sino que «deberán afrontar los dilemas éticos y analizar las ventajas e inconvenientes a través de un proceso de reflexión razonada con base empírica, en lugar de guiarse por la intuición o por criterios aleatorios».

En segundo lugar, el Capítulo II se centra en la «Realización de la IA fiable». Estos requisitos son aplicables a las distintas

⁵³ A este respecto, tal y como destacamos anteriormente, se ha de actuar de un modo preventivo tratando de evitar que se produzcan perjuicios y, para ello, han de establecerse sistemas seguros. Además, en este marco, las personas vulnerables deberían recibir mayor atención y participar en el desarrollo y despliegue de los mismos.

⁵⁴ Por otro lado, al referirse a la equidad, reconoce el documento que existen diversas interpretaciones de este término. No obstante, destaca que en este ámbito ha de tener una dimensión tanto sustantiva como procedimental. La primera de ellas implica, en palabras del texto citado, que se garantice «una distribución justa e igualitaria de los beneficios y costes, y asegurar que las personas y grupos no sufran sesgos injustos, discriminación ni estigmatización». Igualmente, este extremo conlleva que los profesionales respeten el principio de proporcionalidad entre medios y fines. Por su parte, la segunda alude a la «capacidad de oponerse a las decisiones adoptadas por los sistemas de IA y por las personas que los manejan, así como de tratar de obtener compensaciones adecuadas frente a ellas». Con este fin, pues, «se debe poder identificar a la entidad responsable de la decisión y explicar los procesos de adopción de decisiones».

⁵⁵ En otro orden de cosas, la explicabilidad hace referencia a la confianza de los usuarios, para lo cual es necesario que se exija transparencia, es decir, que se comuniquen las capacidades de los sistemas y su finalidad y que las decisiones puedan explicarse a las partes afectadas. Sin embargo, indica que ello no siempre es posible (casos denominados algoritmos de «caja negra»). Por este motivo, «En tales circunstancias, puede ser necesario adoptar otras medidas relacionadas con la explicabilidad (por ejemplo, la trazabilidad, la auditabilidad y la comunicación transparente sobre las prestaciones del sistema), siempre y cuando el sistema en su conjunto respete los derechos fundamentales».

partes intervinientes tales como desarrolladores, responsables del despliegue y usuarios finales, así como la sociedad en su conjunto. Para garantizar estos extremos, el grupo de expertos incorpora la actividad que cada uno de los sujetos referidos ha de desarrollar. Así, prevé que «los desarrolladores deben introducir y aplicar los requisitos de los procesos de diseño y desarrollo», «los responsables del despliegue deben asegurarse de que los sistemas que utilizan y los productos y servicios que ofrecen cumplen los requisitos establecidos» y «los usuarios finales y la sociedad en su conjunto deben permanecer informados sobre dichos requisitos y tener la capacidad de pedir que se cumplan».

Sin entrar en mayor detalle, conviene que, al menos, enumeremos la lista (no exhaustiva) de requisitos (sistémicos, individuales y sociales) que se incluyen y desarrollan en el texto. En este sentido, se contemplan como especialmente importantes los siguientes: la acción y supervisión humana; la solidez técnica y seguridad; la gestión de la privacidad y de los datos; la transparencia; la diversidad, no discriminación y equidad; el bienestar social y ambiental; y la rendición de cuentas. Además, debemos realizar una mención separada al plan de repliegue y seguridad general. A este respecto, indica el grupo de expertos que se han de establecer las salvaguardias necesarias que, en caso de que surjan problemas, se traduzcan en la aplicación del citado plan. Lo anterior, implicará que los sistemas pasen de un procedimiento basado en estadísticas a otro basado en normas, o bien que soliciten la intervención de un operador humano antes de proseguir con sus actuaciones. Igualmente, tal y como se reconoce, el nivel de medidas dependerá, como no puede ser de otro modo, de la magnitud del riesgo que plantee una máquina inteligente.

Por su parte, los métodos técnicos que permiten llevar a cabo una inteligencia artificial fiable pueden traducirse en un conjunto de normas de tipo «lista blanca» (comportamientos que el sistema debería seguir en todo momento) y «lista negra» (restricciones o

estados que jamás tendría que transgredir), así como en combinaciones de ambas. En esta línea, adquiere relevancia la posibilidad de definir indicadores adecuados de calidad «con objeto de garantizar que sea posible saber si dichos sistemas se han ensayado y desarrollado teniendo presentes las consideraciones relativas a la seguridad». En otro orden de cosas, en el campo de los métodos no técnicos debemos reseñar los códigos de conducta y la certificación.

En tercer y último lugar, el Capítulo III está dedicado a la «Evaluación de la IA fiable». Sobre el particular, se ofrece una lista no exhaustiva que es de aplicación directa a los sistemas que interactúen directamente con usuarios y va dirigida, fundamentalmente, a desarrolladores y responsables del despliegue. Esta lista se basa en los siete apartados que anteriormente vimos en relación con los requisitos, anudándose las preguntas que, en su caso, se han de plantear los sujetos intervinientes para asegurar el adecuado funcionamiento. Además, se refiere a la gobernanza de las empresas, organizaciones e instituciones, estableciendo las funciones que han de desempeñar los distintos departamentos que se integren en las mismas.

Tras ello, el grupo de expertos expone algunos ejemplos de oportunidades y preocupaciones principales que plantea la inteligencia artificial. Entre los primeros, cabe destacar la acción por el clima y la necesidad de que se incorpore una infraestructura sostenible, la salud y el bienestar y la educación de calidad y la transformación digital. Por su parte, entre las preocupaciones, se encuentra la identificación y seguimiento de personas, los sistemas encubiertos, la evaluación de ciudadanos vulnerando sus derechos fundamentales y las armas letales autónomas.

En otro orden de cosas, el citado Libro Blanco refiere la necesidad de crear un «ecosistema» de confianza e incide en los riesgos para los derechos fundamentales (en especial, la

protección de datos, la privacidad y la no discriminación⁵⁶). Asimismo, alude a los problemas de seguridad y la necesidad de que el régimen de responsabilidad civil funcione de forma eficaz. A este respecto, se hace necesario reparar en los cambios en el concepto de seguridad y en la necesidad de que siempre exista supervisión humana. Por otro lado, como veremos, los sistemas de inteligencia artificial se han de clasificar según los riesgos que entrañen. Pues bien, para los de alto riesgo contempla una serie de requisitos legales obligatorios y propone, para las que no presenten tal característica, un sistema de etiquetado voluntario.

De esta forma, destaca el citado documento que «Con este sistema, los agentes económicos interesados que no estén sujetos a los requisitos obligatorios pueden optar por someterse, con carácter voluntario, bien a dichos requisitos, bien a un conjunto de requisitos similares, creados de manera específica a los efectos del sistema voluntario. Los agentes económicos interesados obtendrán entonces una etiqueta de calidad para sus aplicaciones de IA». Asimismo, indica que «La etiqueta voluntaria permitirá a los agentes económicos interesados mostrar que los productos y servicios provistos de IA que ofrecen son fiables. Además, permitirá a los usuarios distinguir fácilmente si los productos y servicios en cuestión respetan ciertos referentes objetivos y normalizados a escala de la UE, que van más allá de las obligaciones legales aplicables normalmente. Ello contribuirá a incrementar la confianza de los usuarios en los sistemas de IA y fomentará una adopción generalizada de esta tecnología».

Por su parte, cobra especial relevancia la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías co-

⁵⁶ Sobre el particular, *vid.* VILASAU I SOLANA, M.: «La realización de perfiles y la salvaguardia de los derechos y libertades del afectado», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 181-202.

nexas. Esta norma incluye la denominada «certificación europea de conformidad ética» que, tal y como indica en su Considerando 136, fomentará «la ética por diseño a lo largo de toda la cadena de suministro de los ecosistemas de inteligencia artificial». De esta forma, en la línea de lo que vimos en la etiqueta de calidad prevista en el Libro Blanco, esta certificación adquiere carácter obligatorio para la admisibilidad en los procedimientos de contratación pública en el ámbito de los sistemas de alto riesgo y voluntario para el resto.

Así, en el Anexo que se incorporan las recomendaciones detalladas con respecto al contenido de la propuesta solicitada, se prevé que corresponde a la autoridad de control de cada estado «emitir un certificado europeo de conformidad con los principios éticos y las obligaciones jurídicas tal como se establecen en la propuesta de Reglamento solicitada y el derecho de la Unión pertinente, también como resultado de un proceso de solicitud para cualquier desarrollador, desplegador o usuario de tecnologías no consideradas de alto riesgo que pretenda certificar su conformidad con la propuesta de Reglamento solicitada, según lo desarrollado por la Comisión o cualquier institución, órgano u organismo pertinente de la Unión que pueda designarse en este contexto».

No obstante, a efectos de coordinación a escala de la Unión, la Comisión o cualquier institución, órgano u organismo pertinente de la Unión que pueda designarse en este contexto debe cooperar con la mencionada autoridad de control de cada estado miembro en lo que respecta a la elaboración de un certificado europeo de conformidad con los principios éticos y las obligaciones jurídicas tal como se establecen en la propuesta de Reglamento solicitada y el Derecho pertinente de la Unión, así como el desarrollo de un proceso de solicitud para cualquier desarrollador, desplegador o usuario de tecnologías no consideradas de alto riesgo que pretenda certificar su conformidad con la propuesta de Reglamento solicitada. Siguiendo estas premisas, el artículo 16 de

la Propuesta Reglamento sobre los principios éticos regula este certificado siguiendo las pautas mencionadas.

Por otro lado, debemos hacer referencia, a estos efectos, a la Carta de Derechos Digitales de la ciudadanía española⁵⁷ (que se encuentra en trámites de consulta pública). Así, a pesar de que tendrá que analizarse su valor normativo y su ámbito de aplicación, lo cierto es que en este texto se contemplan derechos de la ciudadanía en sus relaciones con las Administraciones públicas (art. XVI), en el ámbito laboral (art. XVII) o a la protección de la salud en el entorno digital (art. XXI). Sin embargo, el reconocimiento más expreso lo encontramos en el artículo XXIII, que, entre otras cuestiones, destaca la necesidad de que se garantice «el derecho a la no discriminación algorítmica, cualquiera que fuera su origen, causa o naturaleza del sesgo, en relación con las decisiones y procesos basados en algoritmos» o que se asegure la transparencia, auditabilidad, explicabilidad y trazabilidad.

En esta línea, TAPIA HERMIDA⁵⁸ alude a un decálogo de los principios regulatorios de la inteligencia artificial en la Unión Europea. El mismo se concreta en: control de riesgos; protección de los consumidores amplio en sentido subjetivo, geográfico y funcional; seguridad, transparencia y rendición de cuentas; igualdad: prevención de la discriminación automatizada; responsabilidad; imputabilidad; adaptabilidad: adecuación del régimen

⁵⁷ Dicha Carta puede consultarse en:

https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf (fecha última consulta: 03.01.2021).

Sobre los nuevos derechos digitales, BARRIO ANDRÉS, M.: *Manual de Derecho*, cit., p. 168 destaca que tendría que contemplarse una futura «Carta digital» que ofreciera una respuesta a los retos y problemáticas del ámbito digital. A este respecto, señala que, en muchos casos, únicamente sería necesario llevar a cabo una adaptación de los derechos vigentes, pero que, en otras ocasiones, tendrían que reconocerse nuevos derechos, «inaugurando una subsiguiente generación (5G) de derechos fundamentales».

⁵⁸ TAPIA HERMIDA, A.J.: «Decálogo de la inteligencia», cit., pp. 2-7.

de responsabilidad civil a los sistemas de IA de alto riesgo y de riesgo normal; cobertura preventiva; sostenibilidad; y gobernabilidad. Asimismo, a este respecto, interesa resaltar la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre la Ley de servicios digitales y las cuestiones relacionadas con los derechos fundamentales⁵⁹.

En otro orden de cosas, aparece la precitada Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) y que modifica determinadas normas de la Unión, que tiene como finalidad establecer una legislación armonizada para la comercialización, la puesta en servicio y el uso de sistemas de inteligencia artificial en la Unión Europea. Asimismo, incluye 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 video; normas sobre seguimiento y vigilancia del mercado.

En cuanto a las actividades prohibidas, el artículo 5 de la Propuesta mencionada anuda, entre otras, la puesta en el mercado, puesta en servicio o uso de sistemas que desplieguen técnicas subliminales más allá de la conciencia de una persona para distorsionar materialmente su comportamiento de una manera que cause o pueda causarle a esa persona u otra persona daño físico o psicológico o que exploten cualquiera de las vulnerabilidades de un grupo específico de personas debido a su edad, discapacidad física o mental.

⁵⁹ Ley de servicios digitales y cuestiones relacionadas con los derechos fundamentales, 2020/2022(INI), P9_TA(2020)0274.

Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_ES.pdf (fecha última consulta: 03.01.2021).

Por su parte, para los sistemas de alto riesgo articula un conjunto de mecanismos⁶⁰ cuya finalidad última es evitar o, en su caso, reducir los perjuicios causados. Entre otras cuestiones, requiere que se implemente una gestión de riesgos adecuada, que se elabore una documentación técnica que demuestre que cumple con los requisitos legales y que, además, incorporen registros automáticos en los que quede constancia de todos los eventos que se produzcan. Por lo que respecta a la seguridad, se recoge como una medida de apoyo a la innovación la creación de cajas de pruebas (*sandbox*) para proporcionar un entorno controlado que facilite el desarrollo y la validación de sistemas de inteligencia artificial. Además, las medidas previstas no despliegan sus efectos, únicamente, con carácter previo a la comercialización de los productos. Muy al contrario, se contempla un seguimiento posterior (artículo 61 Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021) y la necesidad de que exista un intercambio de información sobre incidentes (o deficiente funcionamiento) entre los proveedores y las autoridades (artículo 62 Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021).

Para lograr los fines propuestos⁶¹, la Propuesta citada prevé la necesidad de que se produzca un trabajo conjunto entre los estados miembros y las instituciones de la Unión Europea. A tal efecto, los primeros han de nombrar una autoridad notificante (artículo 30 Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021), que autorizarán la actividad de los organismos de evaluación de conformidad (artículos

⁶⁰ Así, por ejemplo, el artículo 15 de la citada norma alude a la necesidad de que los sistemas de inteligencia artificial de alto riesgo se diseñen y desarrollen de tal manera que logren, a la luz de su propósito previsto, un nivel apropiado de precisión, solidez y ciberseguridad, y se desempeñen de manera consistente en esos aspectos a lo largo de su ciclo de vida.

⁶¹ Cabe destacar que la Propuesta citada recoge, en sus artículos 71 y 72 una serie de infracciones, sanciones, así como multas administrativas a instituciones, agencias y organismos de la Unión Europea.

31, 32 y 33 Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021). Así, el artículo 59 indica que cada Estado miembro ha de designar las autoridades nacionales competentes que deberán actuar de manera que salvaguarden la objetividad e imparcialidad de sus actividades y tareas.

Por su parte, se prevé la creación de la Junta Europea de Inteligencia artificial (artículos 56 a 58 Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021) que estará formada por las autoridades nacionales y el Supervisor Europeo de Protección de Datos. Además, de conformidad con el artículo 73 de la misma, se otorgan poderes a la Comisión para adoptar actos delegados (que deberá notificar al Parlamento Europeo y al Consejo) y estará asistida por un Comité.

Por último, resta anudar una reflexión a lo anterior. En este sentido, como se ha destacado, las particularidades del ámbito en el que nos movemos pueden justificar la aprobación de unas normas generales de calidad –similares a las ISO–, de tal forma que se establezca un estándar general para los productos y servicios que incorporen inteligencia artificial. De este modo, se evitaría la inseguridad existente en la actualidad y se contribuiría a promover un entorno fiable. Sin duda, ello también repercutiría en la confianza depositada por los potenciales usuarios de esta tecnología. Igualmente, se favorecería la inversión de las organizaciones y empresas lo que, inexorablemente, conllevaría una mejora y continua innovación en este sector. Pues bien, precisamente esta línea ha sido acogida por la mencionada Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) y que modifica determinadas normas de la Unión.

En este sentido, interesa destacar que, en el marco de las obligaciones de los proveedores, el artículo 17 incluye el deber de determinar un sistema de gestión de la calidad. Asimismo, su artículo 43 requiere que los sistemas de alto riesgo se sometan a uno de

los procedimientos de evaluación de conformidad (incluidos en los anexos VI y VII), a excepción de los supuestos previstos en el artículo 47. Además, los organismos de evaluación emitirán certificados que autoricen la actividad de dichos sistemas. Por su parte, es necesario que se redacte una declaración UE de conformidad (como indicativo de que el sistema cumple los requisitos legales) y que el marcado UE de conformidad se coloque de forma visible y legible. Igualmente, el artículo 51 de la norma ordena el registro en la base de datos de la UE de aquellos sistemas de alto riesgo (relacionados en el Anexo III) que se creará, tal y como señala el artículo 60, por la Comisión en colaboración con los estados miembros.

En otro orden de cosas, de una forma similar a lo que indicamos en el ámbito del Libro Blanco y los sistemas de etiquetado voluntario, se incluye en el artículo 69 de la Propuesta la elaboración de unos códigos de conducta destinadas a fomentar la aplicación voluntaria de los requisitos establecidos en la norma a los sistemas de inteligencia artificial distintos de los considerados de alto riesgo.

IV.

EL TRATAMIENTO OFRECIDO POR LAS INSTITUCIONES EUROPEAS A LA RESPONSABILIDAD CIVIL: especial atención a la Resolución del Parlamento Europeo, de 20 de octubre de 2020 y a la propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial

1. CONSIDERACIONES GENERALES

Si recuperamos la anterior reflexión, la primera cuestión a la que debemos enfrentarnos es determinar si, en realidad, las potenciales situaciones que nos encontraremos se pueden resolver en atención a la normativa vigente o si, por el contrario, las máquinas inteligentes presentan rasgos diferenciales suficientes para aprobar unas leyes específicas. A este respecto, no se puede obviar que para el resto de máquinas disponemos de una legislación

adecuada (*vid.* las diferentes normas europeas sobre la materia⁶², así como las distintas regulaciones nacionales). En este sentido, lo cierto es que la consideración de los robots “no autónomos” como productos no genera excesivos problemas, y en consecuencia, la responsabilidad civil derivada por los daños que su uso genere estaría prevista en la vigente normativa reguladora de la responsabilidad por productos defectuosos, esto es, la Directiva 85/374, 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 sus respectivas transposiciones a los ordenamientos nacionales, así como en el resto de regulación europea.

Sin embargo, quizás, no se puede predicar lo mismo con respecto a los daños generados por dispositivos inteligentes que son capaces de tomar decisiones autónomas que escapan del control de los distintos agentes que han participado en su fabricación y desarrollo, acciones independientes que no pudieran ser imputadas a un defecto en la fabricación, no siendo, por tanto, un producto defectuoso.

En este contexto, tenemos que señalar que, tal y como tuvimos ocasión de observar, realmente no estamos ante máquinas totalmente inteligentes y autónomas. Muy al contrario, el rasgo que define a esta tecnología es la ausencia de conocimiento acerca de su funcionamiento. Por lo tanto, el ejercicio se centra en establecer si

⁶² En este sentido, *vid.*, entre otras, la Directiva 85/374, 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; la Directiva 2006/42/CE 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; la Directiva 2009/103/CE relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles; o el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

las precitadas disposiciones son suficientes para resolver los potenciales perjuicios que plantean las novedosas realidades. Desde esta perspectiva, podemos admitir que el marco general que venimos manejando puede mostrarse insuficiente⁶³. Así, descartada la viabilidad de recurrir ante la legislación existente, en abstracto, dos son las posibilidades que aparecen como posibles soluciones.

Por un lado, adaptar dicha normativa a las nuevas realidades para resolver los perjuicios causados. Para llevar esto a cabo se deberían realizar una serie de modificaciones de calado que permitieran la acogida de las tecnologías actuales. En este ámbito, es especialmente relevante la citada Directiva sobre responsabilidad por productos defectuosos. En relación con esta última, como veremos, entre otras cuestiones, se tendría que revisar el concepto de producto defectuoso y su ámbito de aplicación.

A este respecto, con anterioridad a la publicación de la citada Propuesta de Reglamento, lo cierto es que parte de la doctrina consideraba que la Directiva comentada, con una serie de ajustes y adaptaciones, era suficiente para resolver los supuestos de este sector. Asimismo, para aquellos escenarios que se encontraban excluidos, los criterios de responsabilidad civil de la mayoría de los estados eran acordes para este ámbito. Sin embargo, una vez que las instituciones europeas han apostado por otro recurso normativo la conclusión expuesta no parece la más acertada⁶⁴.

⁶³ En este sentido, *vid.* Considerando 3 de la Propuesta de Reglamento incluida en el Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, de 5 de octubre de 2020. Este Informe incluía la citada Propuesta de Reglamento, la Propuesta de Resolución del Parlamento Europeo con recomendaciones a la Comisión sobre un régimen de responsabilidad civil por inteligencia artificial, la Exposición de Motivos, un Anexo con recomendaciones, el Dictamen del Comité de Mercado Interior y Protección del Consumidor (de 7 de julio de 2020) y el Dictamen del Comité de Transporte y Turismo (de 15 de julio de 2020).

⁶⁴ En esta línea, FERREIRA, A.E.: «Partilhar o mundo», *cit.*, p. 25 señala que el sistema legal actual no está preparado para afrontar este tipo de situaciones y que todo ello traerá nuevas formas de pensar la responsabilidad.

Por otro lado, surge la posibilidad de aprobar una normativa diferente y específica para regular estas problemáticas debido a las particularidades que se desprenden de estos sistemas⁶⁵. En este sentido, aparecen tres posibles planteamientos a la hora de afrontar este cometido. En primer lugar, la primera propuesta que se puede realizar es que se apruebe una única disposición o tratado (*hard law*) que englobe todos y cada uno de los supuestos de la práctica. En segundo lugar, cabe recurrir a unos códigos de conducta generales (*soft law*) que sirvan para resolver las distintas problemáticas que podemos encontrar⁶⁶. En tercer lugar, se puede afrontar esta tarea trabajando a nivel de principios, esto es, es-

⁶⁵ A este respecto, parte de la doctrina considera que nos encontramos ante una nueva rama jurídica, a saber, el Derecho de los Robots. En esta línea se manifiesta BARRIO ANDRÉS, M.: «Del Derecho de Internet al Derecho de los Robots», en *Derecho de los Robots* (Dir. M. BARRIO ANDRÉS), Madrid, Wolters Kluwer, 2018, pp. 61-86. Asimismo, ERCILLA GARCÍA, J.: *Normas de Derecho Civil y Robótica. Robots Inteligentes, Personalidad Jurídica, Responsabilidad Civil y Regulación*, Navarra, Aranzadi, 2018, p. 132 prevé que la creación de una personalidad jurídica específica y la atribución de responsabilidad por determinados eventos dañinos implicará por ende la creación de un derecho dedicado a los robots, esto es, de un «Corpus Iuris Robótico».

Igualmente, podemos referir la existencia del denominado «Derecho Digital» que «aspira a ser una nueva disciplina jurídica que nace como consecuencia de tres circunstancias. En primer lugar, la necesidad de contar con una respuesta jurídica precisa para toda actividad relacionada con los servicios de la sociedad de la información –y ahora de la sociedad digital– que disponga de su propia regulación, lenguaje y elementos axiológicos. En segundo lugar, del efecto transversal que las tecnologías, sobre todo Internet, están suponiendo en nuestras vidas y, por ende, en el resto de las tradicionales ramas del Derecho. Y, en tercer lugar, de promulgar algunas normas jurídicas nuevas para dar respuesta a los cambios que introduce la Cuarta Revolución Industrial (o *Industria 4.0*)». En este sentido, *vid.* BARRIO ANDRÉS, M.: *Manual de Derecho, cit.*, pp. 31-32.

⁶⁶ En este sentido, parte de la doctrina señala que los códigos de conducta son insuficientes y que, por tanto, sería necesario ofrecer una regulación por motivos de seguridad jurídica. A este respecto, *vid.* MUÑOZ VILLAREAL, A./GALLEGO CORCHERO, V.: «Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad a los robots», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*

tablecer una suerte de valores generales que sirvan como modelo para ofrecer una solución a los supuestos concretos.

En este escenario, las instituciones europeas han apostado por una vía intermedia. En este sentido, en la Resolución de 20 de octubre de 2020 sobre responsabilidad civil, propone la elaboración de un Reglamento sobre responsabilidad civil en el ámbito de la inteligencia artificial. En dicha norma, se pretenden determinar los principios marco que deberán regir en materia de inteligencia artificial. No obstante, a pesar de que, en la línea de lo destacado, se señala que resulta fundamental que exista una única legislación uniforme en la Unión Europea y que la misma esté basada en principios, mantiene la idea de que la Directiva sobre responsabilidad por productos defectuosos, con una serie de actualizaciones y adaptaciones, es suficiente para ofrecer una solución jurídica a los supuestos de la práctica. En suma, lo que lleva a cabo es añadir una nueva disposición para regular una misma realidad, complicando, más si cabe, la labor del intérprete. Si como hemos visto, precisamente el fundamento para justificar la aprobación de una norma diferente se basa en las particularidades propias del sector, no parece tener excesivo sentido mantener la legislación anterior (con adaptaciones).

A nuestro entender, esta última opción no es todo lo adecuada que sería deseable. En este sentido, nos movemos ante uno de los ámbitos más cambiantes y que más innovación incorpora, lo cual dificulta e imposibilita especificar unos criterios sin que acaben en la obsolescencia. De hecho, esta solución no ha sido factible en otros riesgos tecnológicos. Por ello, debido a la gran variedad de campos de aplicación, consideramos que no es correcto disponer una única norma para regular todas las aplicaciones de la inteligencia artificial. Tal y como se afirma en el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité

(Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, p. 85.

Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020, «las distintas aplicaciones de IA presentan riesgos diferentes». Por este motivo, no parece correcto recurrir a un sistema aplicable a la totalidad de los casos de la práctica, ya que pueden producirse disfuncionalidades.

No obstante, somos conscientes de que no es posible crear tantas normas como supuestos existen y que, quizás no corresponde a la Unión Europea este cometido. Así, proponemos que esta última apruebe un marco general de la inteligencia artificial y que sean los estados miembros los que concreten, respetando el mismo, las leyes y los criterios oportunos. Como quiera que los países integrantes de la Unión Europea difieren tanto en su tradición jurídica como en el contenido de su ordenamiento, lo cierto es que esos principios han de ser lo más amplios posible para que no se produzcan colisiones.

De esta forma, desde nuestra perspectiva, lo más acertado hubiera sido restringir la aplicación de la Directiva de productos defectuosos a los daños generados como consecuencia de máquinas «no inteligentes» y, por su parte, recurrir a la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial (y a las disposiciones nacionales aprobadas, en su caso, como desarrollo de estos principios) para resolver los conflictos derivados de la inteligencia artificial.

En todo caso, como hemos visto, lo cierto es que la citada Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial no parte de esta interpretación. Muy al contrario, a pesar de que introduce un nuevo sistema de responsabilidad civil (con marcadas diferencias), mantiene la vigencia y aplicación de la normativa europea existente y, más específicamente, la referida Directiva. A ello, hay que anudar las distintas disposiciones nacionales reguladoras de la responsabilidad civil, en general, y, en particular, la legislación sobre productos defec-

tuosos, sobre protección de consumidores, etc. Todo este entramado normativo también resulta de aplicación para resolver estos supuestos y determinar, en definitiva, la responsabilidad de los sujetos antes referidos⁶⁷. De esta forma, resulta especialmente complejo concluir acerca de la norma a la que debemos recurrir, ya que no queda claro el ámbito de cada una de las mencionadas disposiciones.

Como tendremos ocasión de comprobar, este extremo no es sencillo de alcanzar por varios motivos. Por un lado, porque la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial se desarrolla a nivel de principios, lo

⁶⁷ A este respecto, uno de los temas fundamentales es la determinación de los sujetos responsables de los daños. Este extremo se puede deducir del Libro Blanco al que anteriormente hicimos referencia, ya que alude a la incertidumbre existente en lo que se refiere a la imputación de responsabilidades entre los distintos agentes económicos de la cadena de suministro. A este respecto, destaca que «En general, la legislación de la UE sobre la seguridad de los productos imputa la responsabilidad al productor del producto comercializado, incluidos todos sus componentes, como los sistemas de IA. Sin embargo, estas normas pueden resultar poco claras cuando la IA es incorporada al producto, una vez que este se ha comercializado, por alguien que no es el productor. Además, la legislación de la UE sobre la responsabilidad civil por los productos regula la responsabilidad de los productores y deja que las normas nacionales en materia de responsabilidad civil se encarguen de los demás participantes en la cadena de suministro».

Asimismo, conviene tener en cuenta que al aproximarnos a estas tecnologías nos encontramos ante una dificultad añadida para determinar el sujeto responsable. En este sentido, a nadie se escapa que muchas de las aplicaciones de la misma requieren de actualizaciones periódicas para mejorar y optimizar su rendimiento e, incluso, para soslayar algún error que incorporaba una versión anterior. En principio, parece que este extremo no entraña ningún inconveniente, ya que, lejos de oscurecer la responsabilidad, facilita su atribución. Y ello, porque se produciría una suerte de transmisión del control y, por tanto, del riesgo sobre la figura del usuario. Sin embargo, esta conclusión no es totalmente acertada y ajustada a la realidad, ya que muchas de las facultades se mantienen en otros sujetos intervinientes, por lo que mantendrían siempre ciertas obligaciones. Esta necesidad de intervención por parte de un tercero podría provocar que, en algún supuesto, nos encontremos ante una concurrencia de culpas.

cual permite un margen más o menos amplio a los estados. Por otro lado, porque el ámbito de aplicación de algunas de las disposiciones referidas puede confluir con el de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. Ello es especialmente perceptible en relación con la Directiva sobre responsabilidad por productos defectuosos. Así, tendremos que llevar a cabo una investigación profunda en este ámbito para dilucidar y definir los contornos de ambas normas.

En todo caso, la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial anuda ciertas reglas que analizaremos para esclarecer esta cuestión. En definitiva, trataremos de resolver la siguiente pregunta: ¿cuándo debemos aplicar la Directiva sobre responsabilidad por productos defectuosos y cuándo la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial? Y, una vez establecida esta correspondencia, tendríamos que ofrecer una solución a las siguientes: ¿quién resulta responsable de los perjuicios? ¿En qué condiciones se manifiesta la responsabilidad civil?

2. LA POSIBLE APLICACIÓN DE LA DIRECTIVA 85/374, DE 25 DE JULIO DE 1985 Y LAS ADAPTACIONES NECESARIAS

En este momento, debemos reflexionar sobre la responsabilidad de los sujetos que intervienen en el proceso de realización, posterior comercialización y utilización de los citados robots inteligentes. A este respecto, la primera consideración de la que debemos partir es que las instituciones europeas entienden que, en principio, disponemos de suficientes normas (tanto a nivel europeo como nacional) para resolver los posibles conflictos de la práctica. No obstante, en un primer momento, en la Resolución del Parlamento Europeo de 16 de febrero de 2017 la propia

Unión Europea se mostró escéptica en relación con la aplicación de la Directiva sobre responsabilidad por productos defectuosos a la responsabilidad civil por los daños que estos sistemas robóticos autónomos e inteligentes pudieran causar. Según reconocía el Parlamento Europeo, el desarrollo por parte de los robots de autonomía y algunos rasgos cognitivos como la habilidad para aprender de la experiencia y tomar decisiones de forma prácticamente independiente puede conllevar que no deban ser considerados como meros objetos en manos de los humanos. Así, proponía que fueran englobados dentro de la categoría de «agentes» capaces de interactuar con su entorno lo que implicaría la necesidad de actualizar la regulación actual por no ser esta adecuada a la nueva realidad tecnológica.

Sin embargo, en la antes citada Comunicación de la Comisión al Parlamento Europeo, de 25 de abril de 2018 y a su documento de acompañamiento, se comenzó a atisbar la posibilidad de aplicar a este ámbito la normativa europea existente⁶⁸. En concreto, la Directiva sobre responsabilidad por productos defectuosos y la Directiva 2006/42/CE 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. Igualmente, en el sector de los vehículos autónomos, la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, En ruta hacia la movi-

⁶⁸ En este sentido, *vid.*, entre otras normas, la Directiva 85/374, 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; la Directiva 2006/42/CE 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; la Directiva 2009/103/CE relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles; o el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

lidad automatizada: estrategia de la UE para la movilidad del futuro, de 15 de mayo de 2018⁶⁹, anuda, a las Directivas mencionadas, la Directiva 2009/103/CE relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles. Por su parte, el Informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies» se manifiesta en idénticos términos, esto es, que las respuestas jurídicas a las problemáticas derivadas del uso de la inteligencia artificial debemos buscarlas en los distintos instrumentos normativos aprobados. Así, por ejemplo, en protección de datos⁷⁰, *vid.* el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Por tanto, se puede inferir que el legislador europeo entiende que dis-

⁶⁹ Este texto se encuentra disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0283&from=EN> (fecha última consulta: 03.01.2021).

⁷⁰ Para más información sobre la protección de datos y su relación con la inteligencia artificial, *vid.* SUMROY, R./DONOVAN, N.: «AI and data protection: balancing tensions», *Practical Law UK Articles*, 2019, pp. 1-16. En este sentido, destacan los autores citados que «A medida que la inteligencia artificial (IA) se vuelve cada vez más popular, las organizaciones están empezando a lidiar con la realidad de cómo equilibrar el diseño y la implementación de la IA con el cumplimiento de la protección de datos. El desafío para las organizaciones que utilizan IA, y que están dentro del alcance del Reglamento general de protección de datos (...) es que varias de las características típicas de la IA parecen, al menos a primera vista, estar en desacuerdo con los principios de la ley de protección de datos».

Además, en este ámbito, cobra especial relevancia la Guía sobre Inteligencia Artificial y Protección de Datos publicada por la Oficina del Comisionado de Información (ICO). La misma se puede visualizar en: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-artificial-intelligence-and-data-protection/> (fecha última consulta: 03.01.2021). Para un estudio sobre la citada Guía, *vid.* BLAIKIE, D./DONOVAN, N.: «New ICO guidance on AI: privacy by design saves retrofitting later», *Practical Law UK Articles*, 2020, pp. 1-4.

ponemos de suficientes normas para abordar la responsabilidad derivada del uso de la inteligencia artificial.

No obstante, el referido Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020, a pesar de que de nuevo incide en la idea de que en la legislación europea y en las normativas nacionales existen criterios para resolver la responsabilidad civil de este ámbito, alude a la necesidad de adaptar ciertas cuestiones. Por ejemplo, la propia definición de producto de la Directiva sobre responsabilidad por los daños causados por productos defectuosos o al requerimiento de que las leyes nacionales faciliten la carga probatoria.

Por su parte, la Resolución de 20 de octubre de 2020 sobre responsabilidad civil, destaca que resulta fundamental que exista una única legislación uniforme en la Unión Europea y que la misma esté basada en principios. A este respecto, señala que la Directiva sobre responsabilidad por productos defectuosos, con una serie de actualizaciones y adaptaciones, es suficiente para ofrecer una solución jurídica a los supuestos de la práctica. No queda claro, pues, en qué circunstancias debemos acudir a estas normas y, en todo caso, que “adaptaciones” son necesarias.

A ello, hay que anudar las distintas disposiciones nacionales⁷¹ reguladoras de la responsabilidad civil, en general, y, en particular, la legislación sobre productos defectuosos, sobre protección de consumidores, etc. Todo este entramado normativo también

⁷¹ En este sentido, GARCÍA TERUEL, R.M.: «El derecho», *cit.*, pp. 1024-1050, analiza la posible aplicación (y, en su caso, las necesarias adaptaciones que se tendrían que adoptar) del Código Civil (arts. 1902 y ss.) y del Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, entre otras normas.

resulta de aplicación para resolver estos supuestos y determinar, en definitiva, la responsabilidad de los sujetos antes indicados.

Por su importancia, nos vamos a referir de forma particular a la Directiva sobre responsabilidad por productos defectuosos⁷². De hecho, es la que más problemática presenta y la que precisa de un análisis para determinar su relación con otras normas. En primer lugar, en la línea de lo destacado en el citado Informe de la Comisión al Parlamento Europeo, de 19 de febrero de 2020, debe reflexionarse sobre el propio concepto de producto defectuoso contenido en el artículo 2 de la Directiva. No hay que perder de vista que, quizás, para ofrecer cobertura a estas tecnologías se tendría que llevar a cabo una revisión, modificación y/o actualización del mismo⁷³.

⁷² Sobre la posible aplicación de esta norma a este ámbito y las necesarias adaptaciones que deberían llevarse a cabo, *vid.* ZURITA MARTÍN, I.: *La responsabilidad*, *cit.*, pp. 79-167.

⁷³ En este sentido, RUBÍ PUIG, A.: «Retos de la inteligencia», *cit.*, pp. 66-67, al plantear la posible aplicación de la Directiva sobre responsabilidad por productos defectuosos a este ámbito, pone de relieve algunos de los inconvenientes que deberían salvarse. A este respecto, en primer lugar, refiere la cuestión relativa al propio concepto de producto que incorpora la citada Directiva, pues no queda claro que, por ejemplo, un *software* no incorporado a un bien mueble queda bajo el amparo del mismo. Como solución plantea una interpretación extensiva de dicha definición. En segundo lugar, se centra en la noción de defecto, ya que «Se pueden plantear dudas acerca de la adecuación de comparar el diseño de una tecnología autónoma con otra de un producto mecánico no automatizado, para cuyo funcionamiento el comportamiento de un individuo sigue siendo crucial». No obstante, destaca que, en muchos supuestos, esta comparación no procederá y bastará con acudir a un «criterio de riesgo-utilidad que compare el diseño del software –el código del algoritmo– con otro alternativo». En tercer y último lugar, se ocupa de la dificultad de aplicar ciertas causas de exoneración debido a que están referidas a los defectos que el producto tenía en el momento de comercialización. No obstante, en el campo de la inteligencia artificial es posible que el mismo no tenga su origen en dicho periodo, sino que se deba a las modificaciones continuas e imprevisibles del sistema realizadas una vez ha sido puesto en el mercado. Sea como fuere, indica el autor referenciado que es muy probable que «muchos productos no dejen de estar durante su vida útil en la es-

En segundo lugar, en cuanto a su ámbito de aplicación, debemos tener en cuenta que queda restringido a ciertas figuras. En este sentido, se centra en la responsabilidad del «productor», entendiendo por tal «la persona que fabrica un producto acabado, que produce una materia prima o que fabrica una parte integrante, y toda aquella persona que se presente como productor poniendo su nombre, marca o cualquier otro signo distintivo en el producto». El resto de los agentes que intervienen en el proceso de elaboración o comercialización quedarían, pues, fuera del ámbito de aplicación de dicha norma y no cabe, en principio, extender el mismo a otros sujetos como el proveedor, el suministrador, el distribuidor, los responsables del servicio, etc.

Además, tampoco las disposiciones nacionales, en la medida que transpongan la citada Directiva, pueden llevar a cabo lo anterior⁷⁴, ni permitir que se indemnicen otros daños no previstos en

fera de control de su fabricante o de uno de los sujetos con el que este estuviera ligado contractualmente».

⁷⁴ Únicamente cabe excepcionar esta regla y, por tanto, permitir un régimen de protección mayor en las legislaciones nacionales cuando, en el momento de notificación de la Directiva, existiera un sistema especial de responsabilidad (art. 13 Directiva sobre responsabilidad por productos defectuosos). Asimismo, el artículo 17 de la misma norma excluye de su ámbito de aplicación aquellos productos que se pongan en circulación antes de la adaptación del ordenamiento jurídico del país de que se trate que, en todo caso, tendrá que llevarse a cabo en el plazo (máximo) de tres años (art. 19 Directiva sobre responsabilidad por productos defectuosos). En concreto, el Considerando 13 de la mencionada norma se refiere a los supuestos en los que «se haya logrado también la protección eficaz del consumidor en el sector de los productos farmacéuticos a través de un régimen especial de responsabilidad», en cuyo caso «deberían seguir siendo igualmente posibles las reclamaciones basadas en dicho régimen».

Sobre el particular, destaca PARRA LUCÁN, M.A.: *Daños por productos y protección del consumidor*, Barcelona, Bosch, 1990, p. 617 que el solamente se tuvo en cuenta, al redactar el citado artículo 13, la ley alemana sobre productos farmacéuticos aprobada en 1976 y, por ello, se aludió en el Considerando 13 expresamente a dichos productos. Igualmente, la misma autora destaca en «La compatibilidad de la directiva de responsabilidad por productos defectuosos y los regímenes de responsabilidad especiales “existentes” en el momento de su

la mencionada Directiva. No obstante, algunos casos han sido resueltos de forma contradictoria a nuestro parecer por el Tribunal de Justicia de la Unión Europea. Así, por ejemplo, se ha negado la posibilidad de que un ordenamiento prevea la responsabilidad del distribuidor de un producto defectuoso en las mismas condiciones que la del productor⁷⁵. Sin embargo, se ha permitido que una legislación nacional atribuya una responsabilidad similar al prestador de servicios que se sirve de productos defectuosos⁷⁶.

En igual sentido, se manifiesta PARRA LUCÁN⁷⁷ cuando señala que esta última solución es muy razonable, pero lo que se cuestiona «es que esto sirva para el prestador de un servicio que utiliza un producto defectuoso y no sirva en cambio, como hemos visto en el apartado anterior, para el distribuidor del producto».

Sea como fuere, como idea fundamental hemos de extraer que la Directiva sobre responsabilidad por productos defectuosos únicamente es aplicable al productor o fabricante y solamente cubre los daños expresamente incluidos en su articulado. Además, los regímenes nacionales que se aprueben a su amparo han de respetar este sistema, sin que quepa ampliar o extender su ámbito a situaciones no previstas. A este respecto, destaca la autora citada⁷⁸ que «La Directiva establece un régimen que imputa la responsabilidad a ciertos sujetos y cubre determinados daños, de modo que,

notificación», *Revista CESCO de Derecho de Consumo*, núm. 13, 2015, p. 136 que, paradójicamente, «no se ve inconveniente en que el propio art. 13 permita que Alemania conserve un régimen “especial” de responsabilidad para los productos farmacéuticos porque “solo” afecta a un sector de producción que es, en definitiva, el sector en el que más reclamaciones se están produciendo entre nosotros en los últimos tiempos».

⁷⁵ Para que sean compatibles, las normas nacionales han de establecer la responsabilidad del distribuidor con base en criterios culpabilísticos o por responsabilidad por vicios. A este respecto, *vid.* SSTJUE 25 abril 2002 (asunto C52/2000); 5 julio 2007 (asunto C-327/2005).

⁷⁶ En este sentido, *vid.* STJUE 21 diciembre 2011 (asunto C-495/2010).

⁷⁷ «La compatibilidad», *cit.*, p. 138.

⁷⁸ *Ibid.*, pp. 141-142.

en este ámbito en el que se ha querido imponer la armonización, fundamentalmente alcanzando soluciones de compromiso entre los sectores afectados, los Estados no pueden mantener ni desarrollar un régimen más beneficioso para las víctimas que permita exigir responsabilidad a otros sujetos ni cubrir la indemnización de todos daños».

De esta suerte, «se frena la tendencia natural de los legisladores y los tribunales nacionales a ampliar la protección de las víctimas de productos defectuosos», y, en todo caso, «Se confirma que la Directiva no es un texto de protección del consumidor sino de establecimiento del mercado interior».

Desde esta perspectiva, hemos de diferenciar entre dos regímenes aplicables cuya aplicación dependerá de la condición del sujeto actuante. Si se trata del productor, acudiremos a la Directiva sobre responsabilidad por productos defectuosos y a las normativas nacionales (de transposición) aprobadas a su amparo. Así, por ejemplo, en España ello se produjo a través de la Ley 22/1994, de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos, cuya vigencia se vio interrumpida el 1 de diciembre de 2007 al ser derogada por el actual Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias⁷⁹.

⁷⁹ El artículo 5 de esta norma señala que se entenderá por productor, sin perjuicio de lo dispuesto en el artículo 138, «al fabricante del bien o al prestador del servicio o su intermediario, o al importador del bien o servicio en el territorio de la Unión Europea, así como a cualquier persona que se presente como tal al indicar en el bien, ya sea en el envase, el envoltorio o cualquier otro elemento de protección o presentación, o servicio su nombre, marca u otro signo distintivo». Por su parte, el citado artículo 138 destaca que se considera productor, además, al fabricante o importador en la Unión Europea de un producto terminado, de cualquier elemento integrado en un producto terminado o de una materia prima. A este respecto, puede dudarse de la adecuación de estos preceptos y de si, en última instancia, esta norma es respetuosa con los mandatos de la Directiva

Por su parte, cuando nos enfrentemos a otros individuos, con los matices que hemos expuesto, debemos recurrir a las disposiciones generales de responsabilidad del ordenamiento jurídico del Estado en cuestión. En nuestro país, esto último implica que tendremos que acudir a los artículos 1101 y siguientes del CC (si se trata de responsabilidad contractual), 1902 y siguientes del CC (en sede de responsabilidad extracontractual), así como a aquellas normativas especiales de responsabilidad vigentes. Así, pues, en este ámbito nos podemos encontrar con diferencias notables de tratamiento en función de la cultura jurídica de la nación en la que se produzca el daño.

Sea como fuere, conviene destacar que el artículo 5 de la Directiva sobre responsabilidad por productos defectuosos contempla una suerte de responsabilidad solitaria entre los sujetos que puedan resultar responsables. Así, señala dicho precepto que «Si, en aplicación de la presente Directiva, dos o más personas fueran responsables del mismo daño, su responsabilidad será solidaria, sin perjuicio de las disposiciones de Derecho interno relativas al derecho a repetir». En esta línea, como tendremos ocasión de comprobar, la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial prevé un régimen similar.

En cuanto al criterio de imputación, estamos ante una responsabilidad objetiva, esto es, que no atiende a la culpabilidad. En este sentido, la Directiva sobre responsabilidad por productos defectuosos señala que «únicamente el criterio de la responsabilidad objetiva del productor permite resolver el problema, tan propio de una época de creciente tecnicismo como la nuestra, del justo reparto de los riesgos inherentes a la producción técnica moderna». Sin embargo, consideramos que esta opción no es todo lo adecuada que sería deseable, ya que solamente prevé el resarcimiento de los perjuicios ocasionados cuando el damnificado pue-

sobre responsabilidad por productos defectuosos y con la doctrina emanada del Tribunal de Justicia de la Unión Europea sobre la materia.

da demostrar el daño real, el defecto del producto y la relación de causa a efecto entre ambos (art. 4 de la citada Directiva). Es decir, es el perjudicado quien tiene que probar el defecto del producto, algo que es extraordinariamente complejo en sistemas robóticos avanzados, lo que hace que se convierta en una prueba diabólica o imposible.

A este respecto, su artículo 128 destaca que «Todo perjudicado tiene derecho a ser indemnizado en los términos establecidos en este Libro por los daños o perjuicios causados por los bienes o servicios». Por su parte, en esta misma línea el artículo 132 del precitado Real Decreto Legislativo 1/2007 prevé que «Las personas responsables del mismo daño por aplicación de este libro lo serán solidariamente ante los perjudicados. El que hubiera respondido ante el perjudicado tendrá derecho a repetir frente a los otros responsables, según su participación en la causación del daño».

Por su parte, las causas de exoneración se prevén en el artículo 7 de la Directiva. Estas últimas dependen de que el productor pruebe: que no se había puesto el producto en circulación; que sea probable que el defecto no existía en el momento de ponerlo en circulación; que el producto no se fabricó para ser vendido o distribuido con fines económicos y que no se realizó en el ámbito de su actividad profesional; que el defecto se debe a que el producto se ajusta a normas imperativas dictadas por poderes públicos; que, en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto; o que, en el caso del fabricante de una parte integrante, el defecto sea imputable al diseño del producto a que se ha incorporado o a las instrucciones dadas por el fabricante del producto. Como se puede comprobar, encontramos, entre otras, una expresión legal del estado de la ciencia para eximir la responsabilidad⁸⁰.

⁸⁰ Sin embargo, el artículo 15.1 b) permite que los estados dispongan «en su legislación que el productor sea responsable incluso si demostrara que, en

Por otro lado, el artículo 8.1 de la misma norma no permite que se limite la responsabilidad del productor «cuando el daño haya sido causado conjuntamente por un defecto del producto y por la intervención de un tercero». A *sensu contrario*, ello sí será posible cuando el perjuicio sea consecuencia, exclusivamente, de dicha intervención por un tercero. Sin embargo, sí se incluye la reducción e, incluso exención, de la responsabilidad cuando el daño se deba, conjuntamente, a un defecto del producto y a la culpa del perjudicado (o de una persona de la que sea responsable el mismo). Asimismo, conviene tener en cuenta que el artículo 12 no permite que se reduzca o elimine la misma a través de cláusulas limitativas o exoneratorias.

En otro orden de cosas, los tipos de perjuicios indemnizables se recogen en el artículo 9 de la Directiva y se concretan en los daños por muerte o lesiones corporales o a una cosa. En este último supuesto, se exige que dicha cosa sea de las que normalmente se destinan al uso o consumo privados y que la víctima lo haya empleado para tales fines. En todo caso, se deducirá una franquicia de 500 ECUS (cuyo equivalente son 16,85 €). Además, se permite que las disposiciones nacionales contemplen lesiones inmateriales (morales), tal y como realiza el artículo 128 del Real Decreto Legislativo 1/2007.

Igualmente, la Directiva contempla la posibilidad de que los estados incorporen límites económicos a las indemnizaciones globales por la muerte o lesiones corporales causadas por artículos

el momento en que él puso el producto en circulación, el estado de los conocimientos técnicos y científicos no permitía detectar la existencia del defecto». En este caso, dicho país deberá comunicar a la Comisión el texto de la medida propuesta, esta informará de ello a los demás Estados miembros y se iniciará un procedimiento especial previsto en la norma (art. 15.2 Directiva). En esta línea, el artículo 140.3 del Real Decreto Legislativo 1/2007 destaca que la causa existente referida al estado de los conocimientos científicos y técnicos no es aplicable a daños producidos por «medicamentos, alimentos o productos alimentarios destinados al consumo humano».

idénticos que presenten el mismo defecto. No obstante, la cantidad que se prevea no podrá ser inferior a 70 millones de ECUS (algo menos de 2.400.000 €).

Por otro lado, debemos referirnos al plazo de prescripción. A este respecto, el artículo 10.1 de la Directiva establece que será de tres años a partir de la fecha en que el demandante tuvo, o debería haber tenido, conocimiento del daño, del defecto y de la identidad del productor. Sin embargo, el periodo para que la víctima tenga conocimiento del perjuicio no es *intemporalis*. Muy al contrario, el artículo 11 de la misma norma señala que los derechos conferidos al perjudicado se extinguirán transcurrido el plazo de diez años a partir de la fecha en que el productor hubiera puesto en circulación el producto (salvo que hubiera ejercitado una acción judicial contra el productor).

Por último, conviene añadir una última reflexión. En este sentido, el artículo 14 de la Directiva excluye expresamente de su ámbito de aplicación los daños que resulten de accidentes nucleares y que estén cubiertos por convenios internacionales ratificados por los Estados miembros. Por este motivo, si la inteligencia artificial se incorpora en tipo de actividades no es posible acudir a la citada disposición para dirimir la responsabilidad del productor. Para tal fin, habrá que estar a la normativa específica, a saber, entre otras, la Directiva 2014/87/Euratom del Consejo, de 8 de julio de 2014, que modifica la Directiva 2009/71/Euratom, de 25 de junio de 2009.

En España, cabe reseñar la Ley 25/1964, de 29 de abril, sobre Energía Nuclear, el Decreto 2177/1967, de 22 de julio, por el que se aprueba el Reglamento sobre Cobertura de Riesgos Nucleares, la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear (reformada por la Ley 33/2007, de 7 de noviembre), la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos y el Real Decreto 1400/2018, de 23 de noviembre, por el que se

aprueba el Reglamento sobre seguridad nuclear en instalaciones nucleares.

3. LA PROPUESTA DE REGLAMENTO SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE INTELIGENCIA ARTIFICIAL

3.1. **Ámbito subjetivo de aplicación: la figura del «operador»**

Como punto de partida, hemos de tener en cuenta que el artículo 1 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial restringe su ámbito de aplicación a las reclamaciones de responsabilidad civil que se produzcan contra los «operadores⁸¹» de sistemas de inteligencia ar-

⁸¹ A este respecto, conviene tener en cuenta que la precitada Resolución del Parlamento Europeo de 16 de febrero de 2017 no aludía a esta figura, sino que incorporaba la del «formador». Este último, aparecía como el encargado de “educar” al robot, esto es, de colaborar en el aprendizaje del mismo. Desde esta perspectiva, señalaba que para poder concluir quién ha de hacerse cargo del daño producido por la máquina inteligente se ha de tener presente el grado de formación del robot. Así, a medida que esta última aumente, también debería ser mayor la responsabilidad del sujeto. En este punto, nos podíamos encontrar, pues, ante una limitación (o, incluso, una exención) de la responsabilidad de otros posibles intervinientes y una translación de la misma al «formador». Sin embargo, en resoluciones posteriores, el legislador europeo pareció olvidar este extremo y no existe otra referencia a este sujeto. En esta línea, el informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies» anuda la persona del «operador». Sea como fuere, la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial incorpora un concepto amplio de «operador», de tal suerte que podemos concluir que la primera acepción de «operador final» se corresponde con la de «operador» a la que alude el Informe del grupo de expertos y, por su parte, el

tificial. En esta misma línea, su artículo 2.1 prevé que esta norma se empleará para resolver los «casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable».

De hecho, esta posición se refuerza en el apartado tercero del mencionado precepto, ya que establece la compatibilidad con otras demandas que se produzcan en materia de responsabilidad civil (como la derivada de la Directiva sobre responsabilidad por productos defectuosos). Además, la Resolución recoge un concepto de «operador⁸²» más amplio que el previsto en otros textos anteriores, ya que se refiere tanto al «operador final», esto es, «la persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento», como al «operador inicial», es decir, «la persona física o jurídica que define, de forma continuada, las características de la tecnología, proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA».

La conclusión, por tanto, parece relativamente sencilla. Siempre que nos encontremos ante un «operador» (ya sea inicial, ya final) adquirirá vigencia la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. Sin embargo, esta interpretación admite dos matices.

«operador inicial» parece que se vincula a la figura del «formador» incluida en la Resolución de 16 de febrero de 2017.

⁸² Hay que tener en cuenta que esta figura aparecía en la Propuesta de Resolución del Parlamento Europeo con recomendaciones a la Comisión sobre un régimen de responsabilidad civil por inteligencia artificial, pero se aludía al operador de interfaz y al operador de *backend* (de servidor).

Desde esta perspectiva, en primer lugar, surge la duda de si estamos ante varios sujetos o si, por el contrario, se pueden reunir ambas condiciones en una misma persona. A este respecto, cabe destacar que, en realidad, ambos supuestos son posibles en la práctica, esto es, en algunas situaciones nos encontraremos ante un «operador inicial» y ante un «operador final» y, por su parte, en otras, tendremos un único operador. En estos últimos casos, dicho operador se beneficiará del funcionamiento del sistema de inteligencia artificial y, además, ejercerá un control directo sobre el mismo, definiendo sus caracteres básicos y proporcionando datos. Esta conclusión viene avalada por la propia Propuesta de Reglamento referida, ya que en su artículo 11 se menciona la posibilidad de que solamente exista un operador.

En segundo lugar, se plantea la disquisición acerca de la relación con el resto de personas intervinientes y que son de sobra conocidos (productor, fabricante, programador, suministrador, responsable del servicio, usuario, etc.). En definitiva, se trata de dilucidar si nos encontramos ante sujetos distintos y separados o si, en algún supuesto, pueden concurrir varias realidades en un mismo individuo. En este sentido, lo cierto es que el «operador inicial» puede coincidir, en ciertos escenarios, con las figuras del fabricante o del productor, cuando estos continúan ejerciendo algún tipo de control sobre el sistema. Por su parte, el «operador final» también es posible que se identifique con el productor, fabricante o programador en los casos en los que, por ejemplo, son los encargados de introducir los datos necesarios a la máquina. Asimismo, cabe que este último operador se confunda con otras personas tales como el usuario, el poseedor o el propietario del robot.

Como se puede comprobar, no es sencillo determinar la normativa aplicable y sería necesario esclarecer cómo se conjugan ambos regímenes, ya que no parece que por el mero hecho de tratarse de un «operador» se deba recurrir a la Propuesta de Reglamento. Máxime, cuando este último posee, a su vez, otras

condiciones reservadas, en principio, para otras normas. Veamos cada uno de los escenarios.

3.1.1. *Relaciones entre operador y productor o fabricante*

Tal y como se ha señalado, existirán supuestos en los que estemos ante un «operador-productor» y otros en los que estas dos realidades residan en dos personas diferentes (como se deduce de algunos preceptos de la Propuesta de Reglamento mencionada como el artículo 8.4⁸³ o el artículo 11). Esta última posibilidad no genera mayores inconvenientes, más allá de la posible injusticia derivada de la aplicación de dos regímenes diferentes de responsabilidad por la mera condición del sujeto actuante.

Más enjundia plantean los casos en los que ambas condiciones concurren en un único sujeto. Y ello, porque pueden surgir dudas acerca de la norma aplicable a las demandas presentadas en este sector. Sobre el particular, se pueden plantear, al menos, tres posibles soluciones. La primera, en la que se entienda que se ha de recurrir a la Directiva sobre responsabilidad por productos defectuosos porque, al margen de las peculiaridades, quedan englobados dentro de su campo de actuación. La segunda, que se considere que la ley aplicable es la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial (entendiendo por tal, en su caso, el futuro Reglamento) por dos motivos. Por un lado, por la categoría especial de operador que supone una distinción con respecto a otros intervinientes y cuyas características particulares aconsejan la aprobación de una ley propia. Por otro lado y derivado de lo anterior, porque este “conflicto” de normas se ha de resolver siguiendo la máxima expresada en el aforismo latino *lex specialis derogat generali*. En suma,

⁸³ Así, el artículo señalado se ocupa de las obligaciones de cooperación y de facilitación de la información del productor para determinar las responsabilidades oportunas, que pueden surgir a petición del operador o de la persona afectada.

ello conlleva que no tendremos que aplicar la disposición general cuando dispongamos de una especial (reguladora de un caso concreto), pasando a ocupar la primera un papel secundario de supletoriedad y de subsidiariedad.

Por último, la tercera (que es la mantenida en la citada Propuesta de Reglamento) opta por un sistema dual –híbrido– en el cual se diferencia entre las dos acepciones de operador a las que hacíamos referencia anteriormente. En este sentido, el artículo 11 de la mencionada Propuesta de Reglamento señala tres reglas, a saber:

- Si el operador inicial también tiene la condición de productor: será de aplicación la Directiva sobre responsabilidad por productos defectuosos⁸⁴.
- Si el operador final es también el productor: prevalecerá la Propuesta de Reglamento.
- Si solo hay un operador y dicho operador es también el productor: prevalecerá la Propuesta de Reglamento.

Como se puede comprobar, nos encontramos ante dos regímenes diferentes entre los que existen distinciones de calado. Desde el plazo de prescripción (significativamente más amplio en la Propuesta de Reglamento citada), pasando por las causas eximentes, hasta el propio criterio de imputación (ya que la Directiva no contempla la clasificación entre sistemas y, por ello, la posibilidad de recurrir a un sistema subjetivo de responsabilidad). Además, estas distinciones pueden verse aumentadas si atendemos al margen de disponibilidad que permite, en algunos puntos, la mencionada Directiva a la hora de transponer su contenido por los estados. Este extremo puede desembocar, sin duda, en una

⁸⁴ Igualmente, esta conclusión se ve reforzada si atendemos al artículo 3 letra d) de la Propuesta de Reglamento, ya que al definir la figura del «operador» señala que lo será «tanto el operador final como el inicial, siempre que la responsabilidad civil de este último no esté ya cubierta por la Directiva 85/374/CEE».

multiplicidad de regulaciones con disparidad de criterios y, por ende, en una grave inseguridad jurídica. Tal hecho repercutirá, inexorablemente, en la inversión que las compañías realicen en este sector (que puede verse gravemente reducida) y provocará que opten por las naciones que incluyan un régimen más laxo de responsabilidad. En suma, contribuirá a llevar a cabo una suerte de mercantilización del sector, que no aparece, al menos *a priori*, como la opción más aconsejable.

3.1.2. *Relaciones entre operador y otros sujetos intervinientes*

Como hemos destacado, también en este caso nos podemos encontrar ante personas diferentes o ante un único operador que desempeñe las funciones de programador, distribuidor e, incluso, que se trate del usuario, poseedor o propietario de la máquina. Asimismo, al margen de la dualidad de sistemas aplicables, tampoco el primer supuesto genera mayor problemática. Situación distinta se produce en el segundo donde es posible imaginar un conflicto de normas. En este marco, no resulta aplicable (como vimos) la Directiva sobre responsabilidad por productos defectuosos, sino que hemos de acudir a las distintas legislaciones nacionales sobre la materia.

Este escenario viene reflejado, de alguna forma, en el artículo 2.3 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial, al destacar la compatibilidad del mismo con «cualquier otra demanda en materia de responsabilidad civil derivada de las relaciones contractuales, así como de la normativa sobre responsabilidad por los daños causados por productos defectuosos, la protección de los consumidores, la lucha contra la discriminación y la protección laboral y del medio ambiente, entre el operador y la persona física o jurídica que haya sufrido un daño o perjuicio a causa del sistema de IA y de que se pueda presentar contra el operador de conformidad con el Derecho de la Unión o nacional».

La posible confluencia de disposiciones y, por tanto, de pugna entre ambas, queda resuelta, no obstante, en la misma Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. En primer lugar, al tratar la responsabilidad de los sistemas de alto riesgo, el artículo 4.5 de la mencionada norma prevé que esta Propuesta de Reglamento «prevalecerá sobre los regímenes nacionales de responsabilidad civil en caso de clasificación divergente por responsabilidad objetiva de los sistemas de IA». Por su parte, cuando regula el resto de sistemas de inteligencia artificial, su artículo 9 indica que las demandas estarán sujetas «en relación con los plazos de prescripción, así como con los importes y el alcance de la indemnización, a la legislación del Estado miembro en el que se haya producido el daño o perjuicio». De lo anterior, podemos extraer las siguientes ideas:

- Si se trata de un sistema de alto riesgo y existen divergencias con las legislaciones nacionales: prevalecerá la Propuesta de Reglamento.
- Si se trata de un sistema no considerado de alto riesgo:
 - o En cuanto a plazos de prescripción, importes y alcance de indemnización: se aplicarán las normas de los estados.
 - o Por lo que respecta al resto de cuestiones (como, por ejemplo, el criterio de imputación o las causas eximentes): se aplicará la Propuesta de Reglamento.

De nuevo, nos encontramos ante distintas normas y diferentes criterios lo que desemboca en una oscuridad y desconocimiento total. Tráiganse aquí las reflexiones que realizamos anteriormente, ya que muchas de las conclusiones son extrapolables, *mutatis mutandi*, en este momento.

Además, tal y como se ha tenido ocasión de señalar, el «operador final» bien puede ser el propietario (que, a su vez, sea consu-

midor o usuario) del robot⁸⁵. En este sentido, conviene tener en cuenta que el Considerando 19 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial se señala que «Dado que el grado de sofisticación de los operadores puede variar en función de si son meros consumidores o profesionales, los deberes de diligencia deben adaptarse en consecuencia». En principio, el deber de diligencia únicamente adquiere relevancia en relación con los sistemas que no sean considerados de alto riesgo, ya que el criterio de imputación reside en la culpa. A este respecto, debemos tener en cuenta que este extremo puede suavizar las obligaciones que analizamos y, con ello, la posible responsabilidad. Asimismo, a pesar de que para los sistemas de alto riesgo se establezca un régimen objetivo⁸⁶, no es cierto que no sea relevante la diligencia empleada por el operador. Por ejemplo, esto último será importante para valorar las causas de exoneración.

⁸⁵ De alguna forma, en tales escenarios nos encontramos ante la figura del «prosumidor», que se produce cuando un sujeto actúa tanto como consumidor como productor. Por ello, es posible que se generen conflictos especiales en este ámbito, ya que este sujeto podría ostentar tres categorías: la de consumidor, la de productor y la de operador. De esta suerte, las normas aplicables serían, en principio, tanto la Propuesta de Reglamento, como la Directiva sobre responsabilidad por productos defectuosos y las normas nacionales. Tendremos que acudir a las reglas señaladas anteriormente para, según los casos, analizar las características concretas y dilucidar la disposición que adquiere vigencia.

⁸⁶ A este respecto, no se puede obviar que la regla general del Derecho español es la responsabilidad subjetiva, esto es, por culpa. Además, nuestro sistema parte de que la carga probatoria recae en el que alega (el demandante), por lo que este último es el que tiene que demostrar cada uno de los elementos de la responsabilidad. No obstante, en determinados casos está justificado que se recurra a un régimen objetivo como, por ejemplo, cuando se trate de actividades peligrosas o en aquellos en los que sea socialmente deseable incidir en dicho sector. En este sentido, *vid.* RUBÍ PUIG, A.: «Retos de la inteligencia», *cit.*, pp. 60-61.

Igualmente, disponemos de otros mecanismos como la inversión del *onus probandi* (a lo que se le denomina responsabilidad cuasi objetiva cuya finalidad es facilitar el resarcimiento a la víctima. Desde esta perspectiva, debemos examinar si, en el ámbito de la inteligencia artificial, existen suficientes motivos para establecer una de estas excepciones.

No se puede obviar que la intervención del propietario adquiere relevancia en relación con su interacción con las máquinas en general (respeto de las normas cuidado o mantenimiento de las mismas) y, con la inteligencia artificial en particular (por la necesidad de incorporar, por ejemplo, actualizaciones). Sin embargo, no se debe perder de vista que, en la línea de lo destacado en la Propuesta de Reglamento, el nivel de formación y de conocimientos exigible a los consumidores y usuarios no puede ser, en ningún punto, equivalente al de los profesionales del ramo. Ello no quiere decir que no podamos encontrarnos ante supuestos, incluso, de concurrencia de culpas, pero este extremo no es óbice para que recurramos a un régimen menos estricto para este colectivo. Precisamente, sobre estas cuestiones incide la Resolución del Parlamento Europeo, de 12 de febrero de 2020, sobre los procesos automatizados de toma de decisiones⁸⁷, al destacar que «cuando estén interactuando con un sistema que automatice la toma de decisiones, se debe informar debidamente a los consumidores de su funcionamiento, de la manera de contactar con un ser humano con poder de decisión y de cómo se pueden verificar y corregir las decisiones del sistema».

En esta misma línea, la Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) prevé, en su artículo 13, que los sistemas

⁸⁷ Procesos automatizados de toma de decisiones: garantizar la protección de los consumidores y la libre circulación de bienes y servicios, 2019/2915(RSP), P9_TA(2020)0032. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0032_ES.pdf (fecha última consulta: 03.01.2021).

Igualmente, cabe destacar la Directiva (UE) 2019/2161, del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L2161> (fecha última consulta: 03.01.2021).

de alto riesgo han de garantizar que su funcionamiento sea lo suficientemente transparente para permitir a los usuarios interpretar la salida del sistema y utilizarla de forma adecuada y, en todo caso, han de ir acompañados de instrucciones de uso en un formato digital apropiado que sea comprendido por estos últimos.

3.2. La necesidad de concretar un ámbito material de aplicación

En este momento y a pesar de que el legislador europeo no lleva a cabo una reflexión en el sentido que proponemos, entendemos que es necesario realizar una apreciación referida al ámbito de aplicación material de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial citada. En este sentido, como hemos visto, únicamente se han establecido dos criterios para delimitar el mismo, a saber, la figura del «operador» y la clasificación entre sistemas de alto riesgo y otros sistemas de inteligencia artificial. Sin embargo, olvida, a nuestro parecer, una cuestión principal y, quizás, más relevante que las anteriores. A este respecto, la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial debería diferenciar entre tipos de daños para concluir cuándo aplicar esta disposición. Así, existen perjuicios que son predicables de todas las máquinas, con independencia de que incorporen o no esta tecnología. Por su parte, otros derivarán, precisamente, de un mal funcionamiento de la inteligencia artificial, ya sea por un error de programación, de actualización o de otra clase.

Si atendemos al artículo 2.1 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial, debemos acudir a la misma para resolver ambos conflictos, ya que señala que «se aplica en el territorio de la Unión a aquellos casos en que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA haya causado daños o perjuicios a la vida, la salud, la integridad física de una persona

física y los bienes de una persona física o jurídica, o bien haya causado daños morales considerables que den lugar a una pérdida económica comprobable». No diferencia, pues, entre unos y otros ni matiza esta cuestión. A igual conclusión llegamos si analizamos el artículo 3 letra i), ya que señala que será «daño o perjuicio» el «impacto adverso que afecta a la vida, la salud, la integridad física de una persona física, los bienes de una persona física o jurídica o bien que produce daños morales significativos que resultan en una pérdida económica comprobable».

Pues bien, si el evento dañoso no se ha producido como consecuencia de la inteligencia artificial o esta misma no ha influido en algún aspecto (contribuyendo a aumentar el menoscabo), no está justificado recurrir a un régimen especial como el previsto en la referida Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. Para tales escenarios, la normativa vigente (Directiva sobre responsabilidad por productos defectuosos y las disposiciones de los estados) es suficiente y no cabe excepcionar su empleo. Esta controversia podría solventarse anudando un inciso final al precitado artículo 2.1 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial como el que a continuación se refiere: «como consecuencia del empleo de dicha inteligencia artificial o contribuyendo la misma, de alguna forma, a su causación».

En otras palabras, desde nuestra perspectiva, lo más correcto sería diferenciar entre dos tipos de daños. De un lado, aquellos daños que son predicables de todas las máquinas, con independencia de que incorporen sistemas de *machine learning* y, de otro lado, aquellos que son específicos de dicha tecnología. Así, existen perjuicios que pueden producirse en el seno de cualquier robot como, por ejemplo, una explosión, la incorporación de un material dañino, etc. Por su parte, otros se deben a la propia incorporación de las modernas tecnologías o como consecuencia de tal hecho. Imagínese, por ejemplo, que la red neuronal y los algoritmos que integra, al interpretar los datos proporcionados,

comete un error debido a que ciertos *inputs* no son adecuados. A este respecto, consideramos que la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial únicamente debería emplearse para estos últimos escenarios y que, el resto de los supuestos quedarían bajo el amparo de la Directiva sobre responsabilidad por productos defectuosos u otras normas de responsabilidad.

Asimismo, tampoco se debería tener en cuenta este extremo para realizar la clasificación entre sistemas a la que nos referiremos posteriormente, ya que se estarían incluyendo riesgos que no son, propiamente, de la inteligencia artificial. Máxime, porque la posibilidad de que se produzca una situación como la descrita (de explosión) sería predicable de todos los que se incorporen a un soporte físico. Esta contingencia únicamente encontraría fundamento si se extiende dicha clasificación para todas y cada una de las máquinas existentes, algo que no es probable que ocurra y tampoco queda claro si sería, de ser adoptada, la solución óptima.

3.3. La clasificación de los sistemas de inteligencia artificial

A pesar de que pueden establecerse múltiples clasificaciones de los sistemas que incorporan inteligencia artificial, desde nuestra perspectiva son especialmente relevantes dos. En primer lugar, debemos tener en cuenta el criterio del nivel de autonomía con el que interviene la máquina. De otro lado, se han de catalogar atendiendo a los riesgos potenciales, es decir, a la posibilidad de causar daños y los tipos de perjuicio.

3.3.1. El nivel de autonomía de los sistemas: la atribución de personalidad jurídica

Desde el ámbito de la pretendida autonomía de las máquinas inteligentes, lo cierto es que podemos establecer una suerte de clasificación que atienda a la propia capacidad de las mismas para

actuar de forma racional, aprender y tomar decisiones de forma independiente. A este respecto, ya señalamos anteriormente que no nos encontramos en un estadio suficiente para referir esta realidad y que no podía aludirse, en puridad, a la inteligencia artificial ni a las actuaciones autónomas. Sea como fuere, ello no quiere decir que este extremo no sea relevante para plantear, en un futuro, estas cuestiones y analizar, por tanto, la viabilidad de atribuir personalidad jurídica a estos sistemas y, por ende, responsabilidad civil.

En este sentido, inicialmente, la Resolución de 16 de febrero de 2017 contempló esta posibilidad. Así, señaló que, debido a la situación en la que se encontraba la humanidad en la que la inteligencia artificial parecía decidida «a desencadenar una nueva revolución industrial», resultaba de vital importancia ponderar las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación. Por todo ello, destacó que, a pesar de que en la etapa actual no es posible atribuir la responsabilidad a esta última, debiendo recaer en un humano, ello no es óbice para que, en un momento posterior, sí quepa realizar este ejercicio. En esta línea, señaló que a largo plazo se debería crear «una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente».

No obstante, esta idea ha sido matizada y corregida en otros instrumentos posteriores, quizás por haber observado prudentemente el legislador europeo que se trata de un escenario imposible y poco realista atendiendo al momento que vivimos. A este respecto, el ya citado Informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies⁸⁸», des-

⁸⁸ Asimismo, el citado Informe recoge una serie de retos que plantean las tecnologías. Para un estudio pormenorizado de estas cuestiones, *vid.* GÓMEZ

carta el reconocimiento de esta personalidad jurídica a los robots. Indica, no obstante, que sería posible otorgar la misma, pero requeriría de una reforma legislativa profunda. Por otro lado, más contundente es la citada Resolución de 20 de octubre de 2020 sobre responsabilidad civil, que destaca no es necesario atribuir dicha personalidad a los sistemas de inteligencia artificial, ya que se pueden eludir los problemas haciendo responsables a las diferentes personas de toda la cadena de valor que crean, mantienen o controlan el riesgo asociado. De esta forma, parece que, definitivamente, el Parlamento Europeo ha abandonado la premisa de que, en un futuro, debíamos aspirar a responsabilizar a las máquinas inteligentes de los daños que causasen.

Sea como fuere, debemos ser conscientes de que estamos ante una cuestión que no es, ni mucho menos, pacífica. Las críticas a la posibilidad de reconocer esta personalidad jurídica son abun-

LIGÜERRE, C./GABRIEL GARCÍA-MICÓ, T.: «Liability for Artificial Intelligence and other emerging technologies», *InDret*, núm. 1, 2020, pp. 503-510. Destacan los autores citados que «el derecho europeo dispone de instrumentos normativos que dan respuesta a la pretensión indemnizatoria básica de la víctima de cualquier accidente y que «A esa relativa uniformidad de las reglas de responsabilidad se suman los principios de neutralidad tecnológica y de equivalencia funcional con los que se ha intentado dar respuesta a las nuevas situaciones generadas por el progreso tecnológico: la intervención de la tecnología no debería modificar la aplicación de las reglas existentes (technological neutrality) y las reglas que existen para los daños imputables a un comportamiento humano deben aplicarse a los casos en que tal comportamiento sea muy remoto o indirecto o, incluso, inexistente, pues deben aplicarse las mismas reglas al daño causado por un humano que al que causa una máquina (functional equivalence)». En igual sentido, RUBÍ PUIG, A.: «Retos de la inteligencia», *cit.*, p. 61 indica que «Con arreglo al principio de neutralidad tecnológica, las reglas propias de un ordenamiento jurídico no se habrían de modificar en función de la tecnología sobre la que han de proyectarse. Con arreglo al principio de equivalencia funcional, deberían emplearse las mismas reglas en un ordenamiento jurídico para tratar unos mismos problemas; por ejemplo, las mismas reglas de imputación a un sujeto de un resultado lesivo con independencia de si los daños fueron causados por uno de sus agentes o por el uso de una tecnología autónoma basada en IA».

dantes y variadas⁸⁹. Quizás la más extendida es la que entiende que esta atribución de personalidad se debe a una manifestación más del antropocentrismo. En este sentido, se alude al empeño de “imitar” el funcionamiento del cerebro humano en el seno de los robots inteligentes y de “crear sujetos a su imagen y semejanza”. Asimismo, se hace referencia a los problemas derivados de la necesidad de incorporar un patrimonio propio⁹⁰ y, por tanto, determinar quién ha de financiar dicho gasto. Por otro lado, se indica que no es posible lograr un grado tan alto de autonomía y que, en última instancia, siempre se precisará de la intervención de un humano y quedarán posiciones residuales que manejen cierto control sobre el sistema.

Sin negar lo cierto de las anteriores posiciones, consideramos que estas interpretaciones son acertadas para la realidad actual, pero no cabe extenderlas a los más que posibles escenarios que se producirán. De hecho, la mayoría de los inconvenientes que se alegan se pueden soslayar y, por su parte, otros no desa-

⁸⁹ En este sentido, *vid.* WAGNER, G.: «Robot Liability», en *Liability for Artificial Intelligence and the Internet of Things* (edit. S. LOHSSE/R. SCHULZE/D. STAUDENMEYER), Baden-Baden, Nomos, 2019, pp. 27-62.

⁹⁰ En esta línea, parte de la doctrina se ha mostrado crítica con la Resolución de 20 de octubre de 2020 sobre responsabilidad civil referida anteriormente, ya que ha abandonado dos ideas fundamentales que, por el contrario, sí se recogían en la Resolución del Parlamento Europeo, de 16 de febrero de 2017 (que posteriormente comentaremos), a saber, el establecimiento de fondos de compensación de amplio alcance y la creación de una personalidad jurídica electrónica. En este sentido, entiende que el texto de 2020 carece de la ambición necesaria para un cambio de paradigma en la responsabilidad asociada con las características de los sistemas de inteligencia artificial. Así, recurrir a las soluciones tradicionales de responsabilidad equivaldrá a un retoque insuficiente para garantizar la reparación del daño sufrido por la parte afectada. Por lo tanto, se justifica establecer la responsabilidad de una persona electrónica, lo que, por supuesto, requerirá la construcción de un sistema financiero para esa entidad. A este respecto, *vid.* SOUSA ANTUNES, H.: «Civil liability applicable to artificial intelligence: a preliminary critique of the European Parliament Resolution of 2020», *SSRN*, 2020, pp. 21-22.

parecen negando la personalidad jurídica. Así, por ejemplo, la dificultad de la financiación se produce igualmente con independencia de este extremo. Huelga señalar que las instituciones europeas, conscientes de tal impedimento, se han centrado en ofrecer un tratamiento acorde tanto en el sector del aseguramiento obligatorio como en el establecimiento de fondos de compensación. A ello hay que sumar la multiplicidad de sujetos que intervienen en este proceso y que pueden resultar, potencialmente, responsables. Sin duda, es verdaderamente costoso delimitar las distintas figuras y concluir, en un caso concreto, quién ha de hacerse cargo de la reparación del daño.

Por todo ello, desde nuestra perspectiva, las referidas reflexiones no son todo lo adecuadas que sería deseable. Si bien es cierto que muchos de los sistemas de inteligencia artificial no merecerán la consideración de robots inteligentes y autónomos y, por tanto, no está justificado que se reconozca su personalidad jurídica, ello no es predicable de otros más sofisticados y precisos. En este sentido, a pesar de que no sea posible en estos momentos, con el desarrollo de la tecnología se implementarán máquinas que sean capaces de actuar con un nivel de automatización muy elevado y con gran autonomía. Por este motivo, entendemos que los esfuerzos han de dirigirse a que los citados robots alcancen personalidad jurídica propia⁹¹. Como se ha dicho,

⁹¹ En este sentido, LIN, P./ABNEY, K./BEKEY, G.A.: *Robot Ethics: The Ethical and Social Implications of Robotics*, Massachusetts, The MIT Press, 2012, p. 8 destacan que las leyes de responsabilidad de productos no se han probado en gran medida en robótica y que, a medida que los robots se vuelven más autónomos, puede ser plausible asignar responsabilidad al propio robot.

Igualmente, algunos autores ponen de relieve que «estos robots o “personas ciber físicas” serán capaces de desarrollar una individualidad propia a partir de su interacción independiente con el entorno, por lo que no sería justo imputar las decisiones que tomen estas entidades con base en su propio aprendizaje a sus programadores y fabricantes». Vid. ZAPATA SEVILLA, J.: «Inteligencia artificial y responsabilidad civil: el caso de las organizaciones descentralizadas autónomas», 2019, pp. 2-3. Disponible en:

esta cualidad no podrá predicarse de todos y cada uno de los existentes, pero sí de aquellos más avanzados que puedan aprender y formular, llegado el caso, decisiones por sí mismos⁹². No obstante, para llegar a este grado de autonomía, las máquinas han de situarse en una posición en la que ninguno de los sujetos intervinientes (productor, diseñador, programador, usuario, formador, operador o propietario) puedan conocer o predecir, *a priori*, la opción que escogerá el robot. En tales escenarios, lo cierto es que resulta verdaderamente complejo justificar que deba hacerse cargo del perjuicio una persona que, sencillamente, no posee el control suficiente sobre el sistema por su propia autonomía. Asimismo, esta transformación en el pensamiento generalizado precisa de una modificación en los ámbitos social,

<https://riuma.uma.es/xmlui/bitstream/handle/10630/18645/Inteligencia%20artificial%20y%20responsabilidad%20civil%20Oviedo%20%28Comunicaci%C3%B3n%20Jos%C3%A9%20Zapata%20Sevilla%29.pdf?sequence=1> (fecha última consulta: 03.01.2021).

En contra, NÚÑEZ ZORRILLA, M.C.: «Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial», *Revista española de derecho europeo*, núm. 66, 2018, pp. 9-10 indica que «en ningún momento se les puede atribuir -a los entes con IA- la noción de culpa o de dolo en la comisión de sus actos dañosos, pues estamos partiendo de una voluntad que no se ha formado de manera completamente libre, sino siempre sujeta a su condición de ser dependiente y sometido a la voluntad de otro. Por tal motivo, cuando el robot produce un daño, el sujeto al que debe imputársele la responsabilidad como sujeto en principio culpable, no es al robot, sino a la persona que tiene su control».

⁹² A este respecto, ČERKA, P./GRIGIENĖ, J./SIRBIKYTĖ, G.: «Liability for damages», *cit.*, p. 378 señalan que «si la IA fuera completamente autónoma (como la superinteligencia), entonces deben ser conscientes de sus acciones. Si son conscientes de sus acciones, deben ser responsables de sus acciones. La autonomía legal de IA significa que IA tiene derechos y el correspondiente conjunto de deberes. Por ley, los derechos y deberes se atribuyen a las personas jurídicas, tanto naturales (como las personas) como artificiales (como las sociedades). Por lo tanto, si buscamos que IA sea responsable de sus acciones, debemos atribuirle la personalidad jurídica. Significa que los legisladores deben revisar el marco legal existente y adaptarlo a las necesidades cambiantes de la sociedad».

cultural, ético⁹³ y jurídico⁹⁴ en los distintos países. Las implicaciones del reconocimiento de personalidad exigen un cambio de paradigma y para ello es preciso que se aborden y se superen ciertos debates filosófico-jurídicos.

A pesar de que es posible que, desde un punto de vista teórico, la incorporación de un capital propio a los sistemas de inteligencia artificial puede ser una solución simplista, desde una perspectiva práctica y funcional aparece como la más adecuada. Con este régimen, las víctimas dispondrían de un medio seguro al que acudir para obtener una indemnización acorde y se evitarían los escollos que antes mencionábamos. Tampoco parece que las indi-

⁹³ En este sentido, el artículo 5.1 de la Propuesta de Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas recoge los principios éticos de la inteligencia artificial, la robótica y las tecnologías conexas y destaca que «La inteligencia artificial, la robótica y las tecnologías conexas, incluidos los programas informáticos, los algoritmos y los datos utilizados o producidos por dichas tecnologías, se desarrollarán, desplegarán y utilizarán en la Unión de conformidad con el Derecho de la Unión y respetando plenamente la dignidad, la autonomía y la seguridad humanas, así como otros derechos fundamentales establecidos en la Carta».

⁹⁴ Así, por ejemplo, una de las importantes cuestiones a las cuales ha de ofrecerse una solución adecuada es la relativa a los derechos de propiedad intelectual en el ámbito de la inteligencia artificial. Puede consultarse un estudio al respecto en STEPHENS, K./BOND, T.: «Artificial intelligence: navigating the IP challenges», *Practical Law UK Articles*, 2018, pp. 1-14; KEMP, R./MOYNIHAN, D./KEMP, C.: «IP in AI-generated works, datasets and trade secrets», *Practical Law UK Articles*, 2020, pp. 1-9; XALABARDER, R.: «Inteligencia artificial y propiedad intelectual», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 205-223. Por otro lado, sobre la protección de las marcas, *vid.* CLARK, B./WILKINSON-DUFFY, R.: «AI and trade mark law: keeping up with the robots», *Practical Law UK Articles*, 2020, pp. 1-12.

Igualmente en este ámbito cabe reseñar la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial, 2020/2015(INI), P9_TA(2020)0277. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_ES.pdf (fecha última consulta: 03.01.2021).

caciones sobre el mantenimiento residual del control sean, realmente, aplicables a este sector. Y ello, porque estas problemáticas se presentarán en todos los escenarios posibles, sin que guarde relación directa con la personalidad jurídica.

Una vez sentado lo anterior, entendemos que esta problemática no debe ocupar el papel principal en los debates acerca de las modernas tecnologías. Lógicamente, esto último no quiere decir que se trate de un tema banal o baladí, sino que, sencillamente, tenemos un contexto diferente y que precisa de soluciones basadas en el presente (sin que debamos precipitar los acontecimientos). En este sentido, en una época posterior, seguramente, tendremos que plantearnos estas disquisiciones y otras íntimamente ligadas (como la discusión acerca de la volición y la libertad de estas máquinas, el reconocimiento de una moral propia, etc.). De hecho, en tal contexto, será cuestionable la vigencia de la actual Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial (de ser finalmente aprobada).

3.3.2. *El riesgo como criterio para clasificar los sistemas de inteligencia artificial en los documentos emitidos por las instituciones europeas*

En otro orden de cosas, consideramos que el criterio fundamental para clasificar los sistemas de inteligencia artificial es el riesgo, esto es, el potencial peligro que genera la utilización de estas máquinas. A este respecto, se debe diferenciar entre aquellos sistemas que se consideren de alto riesgo, esto es, en los que la probabilidad de que se produzcan en la práctica es elevada y aquellos otros de los que no cabe predicar tal característica. Como pone de relieve NÚÑEZ ZORRILLA⁹⁵, a pesar de que resulta evidente que «las nuevas tecnologías ofrecen un aspecto sumamente po-

⁹⁵ *Inteligencia artificial y responsabilidad civil*, Madrid, Reus, 2019, p.10.

sitivo en la actividad del ser humano, racionalizando y suprimiendo laboriosos y arriesgados trabajos, y sobre todo rompiendo, tanto en el ámbito laboral como social, las barreras del espacio y el tiempo», con esta evolución «están naciendo nuevas formas de lesionar los derechos, nuevas formas de dañar al ser humano y por qué no, posibles nuevos derechos que deben protegerse».

En esta línea, las instituciones europeas han planteado estas cuestiones a lo largo de sus incursiones en esta materia. Así, en el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020, se comenzó a recabar opiniones acerca del establecimiento de una responsabilidad objetiva y su vinculación con un seguro para aquellas aplicaciones con un perfil de riesgo específico. Precisamente, esta idea ha sido acogida en la precitada Resolución de 20 de octubre de 2020 sobre responsabilidad civil, en la que se considera que el riesgo predicable de los distintos sistemas de inteligencia artificial no es equivalente.

Así, propone un régimen basado en este extremo que deberá regularse de forma exhaustiva. Para los sistemas de alto riesgo (que se enumerarán en el futuro Reglamento sobre responsabilidad civil en materia de inteligencia artificial) «parece razonable establecer un régimen común de responsabilidad objetiva para los sistemas de IA autónomos» (tal y como lleva a cabo el artículo 4.3 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial⁹⁶). Por su parte, los sistemas de inteligencia artificial que no dispongan de tal carácter han de quedar sujetos a la responsabilidad subjetiva pero con una presunción de culpa del operador, esto es, con una inversión del *onus probandi*,

⁹⁶ No obstante, el artículo 5 del Reglamento propuesto prevé una serie de importes máximos que variarán en función del tipo de daño que produzca y el artículo 6 se ocupa del alcance de la indemnización.

de tal forma que si este último quiere eximirse de responsabilidad tendrá que demostrar que ha observado el deber de diligencia (artículo 8 apartados 1 y 2 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial⁹⁷). En cuanto a los sistemas de inteligencia artificial que no hayan sido evaluados por la Comisión y que no estén clasificados se registrarán por la responsabilidad objetiva si han causado incidentes reiterados que den lugar a un daño o un perjuicio grave.

Desde esta perspectiva, en su Considerando 16, prevé la elaboración de una enumeración exhaustiva de los sistemas de inteligencia artificial de alto riesgo que, además, ha de ser revisada «sin demoras injustificadas y, a más tardar, cada seis meses». El Parlamento Europeo es consciente de que nos encontramos ante un ámbito especialmente cambiante y sometido a actualizaciones constantes lo que, sin duda, puede dificultar la anterior tarea. Por este motivo y para evitar correr el riesgo de que las citadas clasificaciones queden obsoletas, es necesario que se proceda a examinar y comprobar que los criterios que se manejaron continúan teniendo vigencia. A tales efectos, se contempla la creación de un comité permanente, «similar al Comité Permanente sobre Precusores o al Comité Técnico sobre Vehículos de Motor ya existentes, que incluyen a expertos nacionales de los Estados miembros y a las partes interesadas». Este último deberá trabajar conjuntamente con la Comisión para llevar a cabo la anterior tarea.

⁹⁷ En este sentido, señala que «El operador no será responsable si puede demostrar que no tuvo culpa en el daño o perjuicio causado, basándose en uno de los siguientes motivos:

a) el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador, o

b) se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles».

En esta línea, el Considerando 14 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial⁹⁸ señala que los citados sistemas han de establecerse en un Anexo al mismo. Sin embargo, a diferencia de los trabajos previos en los que sí aparecía este extremo, el Anexo de la Propuesta no se encuentra completado.

Sea como fuere, la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas⁹⁹ contempla

⁹⁸ En este sentido, destaca el mismo que «En un anexo al Reglamento presente deben enumerarse exhaustivamente todos los sistemas de IA de alto riesgo. Habida cuenta de la rápida evolución técnica y del mercado a escala mundial, así como de los conocimientos técnicos que se necesitan para una revisión adecuada de los sistemas de IA, deben delegarse en la Comisión poderes para adoptar actos delegados con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea con el fin de modificar el presente Reglamento en lo que se refiere a los tipos de sistemas de IA que entrañan un alto riesgo y los sectores críticos en los que se usan. Sobre la base de las definiciones y disposiciones recogidas en el presente Reglamento, la Comisión debe revisar el anexo en el plazo más breve posible y, en todo caso cada seis meses y, si procede, modificarlo mediante actos delegados. La evaluación por parte de la Comisión de si un sistema de IA presenta un riesgo elevado debe comenzar al mismo tiempo que la evaluación de la seguridad de los productos a fin de evitar una situación en la que un sistema de IA de alto riesgo ya esté aprobado para su comercialización pero aún no esté clasificado como de alto riesgo y, por tanto, funcione sin cobertura de seguro obligatoria. Para que las empresas y los organismos de investigación dispongan de seguridad suficiente en términos de planificación e inversión, los cambios en los sectores críticos solo deben realizarse cada doce meses. Debe instarse a los operadores a que informen a la Comisión de si están trabajando en una nueva tecnología, productos o servicios que se inscriban en uno de los sectores críticos existentes previstos en el anexo y que posteriormente podrían clasificarse como sistema de IA de alto riesgo».

⁹⁹ Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012 (INL), P9_TA-PROV(2020)0275.

Esta disposición tanto la Resolución, así como dos anexos: uno con Recomendaciones detalladas respecto al contenido de la propuesta solicitada y la Propuesta Reglamento del Parlamento Europeo y del Consejo, sobre los prin-

una lista exhaustiva y acumulativa de sectores de alto riesgo y de usos o fines de alto riesgo que conllevan un riesgo de violación de los derechos fundamentales y las normas de seguridad. Esta última tendrá importancia para concretar el criterio de imputación aplicable y para exigir un posible seguro de responsabilidad civil. Además, resulta fundamental que se encuentre basada en análisis científicos y probabilísticos y que no se limite a recoger una serie de aspectos arbitrarios e infundados. En este sentido, dicha Resolución diferencia, en la línea de lo destacado, entre sectores de alto riesgo (como el campo del transporte, la asistencia sanitaria, la educación o la seguridad y defensa) y usos o fines de alto riesgo (como los tratamientos y procedimientos médicos, la conducción automatizada o la gestión del tráfico).

Así, el Considerando 11 de la mencionada Resolución señala que, a los efectos de la evaluación de estos sistemas, «deben tenerse en cuenta el sector en el que se desarrollan, despliegan o utilizan, su uso o finalidad específica y la gravedad de la lesión o daño que cabe esperar que se produzca. El grado de gravedad debe determinarse sobre la base de la magnitud de la lesión o daño potencial, el número de personas afectadas, el valor total del perjuicio ocasionado y el daño a la sociedad en su conjunto. Los tipos graves de lesiones y daños son, por ejemplo, las violaciones de los derechos de los niños, los consumidores o los trabajadores que, debido a su alcance, el número de niños, consumidores o trabajadores afectados o su impacto en la sociedad en su conjunto, entrañan un riesgo significativo de vulneración de los derechos fundamentales y las normas de seguridad establecidas en el Derecho de la Unión».

Dejando ello al margen, si las dos Propuestas de Reglamento se aprueban definitivamente, no queda claro la relación existente

cipios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas; y otro que recoge una lista exhaustiva y acumulativa de sectores de alto riesgo y de usos o fines de alto riesgo que conllevan un riesgo de violación de los derechos fundamentales y las normas de seguridad.

entre ambas enumeraciones de sistemas de inteligencia artificial. Máxime, porque es posible que los criterios que se manejan en uno y otro caso difieran. Desde nuestra perspectiva, tanto por la especialidad del ámbito del Derecho de daños como por la propia categoría normativa, el Reglamento tendría preferencia en cuanto a su aplicación. En todo caso, entendemos que las pautas que se manejen para elaborar dicha lista han de ser más concretos y descender, en algún punto, llevando a cabo subdivisiones.

A todo ello, hay que anudar la comentada Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*) que, en su artículo 6, establece una serie de normas para la clasificación de los sistemas de alto riesgo, a saber, que esté destinado a ser utilizado como un componente de seguridad de un producto, o es en sí mismo un producto (cubierto por la legislación de armonización de la Unión enumerada en el Anexo II); que el producto cuyo componente de seguridad es el sistema, o el propio sistema como producto, deba someterse a una evaluación de la conformidad por parte de un tercero con vistas a la comercialización o puesta en servicio de ese producto (de conformidad con la normativa prevista en el Anexo II). Todo ello, con independencia de que el mismo se comercialice.

Asimismo, también tendrán dicho carácter los incluidos en el Anexo III¹⁰⁰, que se concretan en las siguientes áreas: identifi-

¹⁰⁰ En todo caso, como prevé el artículo 7 de la Propuesta, la Comisión está facultada para adoptar actos delegados para actualizar la lista del Anexo III añadiendo sistemas de alto riesgo cuando se cumplan las dos condiciones siguientes: que estén destinados a utilizarse en cualquiera de los ámbitos enumerados en los puntos 1 a 8 del Anexo III; que planteen un riesgo de daño a la salud y seguridad, o un riesgo de impacto adverso sobre los derechos fundamentales, es decir, con respecto a su gravedad y probabilidad de ocurrencia, equivalente o mayor al riesgo de daño o impacto adverso. que plantean los sistemas de alto riesgo ya mencionados en el Anexo III.

cación biométrica y categorización de personas físicas; gestión y operación de infraestructura crítica (tráfico rodado y suministro de agua, gas, calefacción y electricidad); educación y formación profesional; empleo, gestión de trabajadores y acceso al autoempleo; acceso y disfrute de servicios privados esenciales y servicios y beneficios públicos; cumplimiento de la ley (entre otros, los utilizados por las autoridades encargadas de hacer cumplir la ley para realizar evaluaciones individuales de riesgo de cometer un delito por parte de personas físicas, o a ser usados por las autoridades policiales como polígrafos y herramientas similares o para detectar el estado emocional de una persona física); gestión de migración, asilo y control de fronteras; y administración de justicia y procesos democráticos.

3.3.3. *Reflexiones acerca de la correcta clasificación de los sistemas de inteligencia artificial*

Como se tuvo ocasión de señalar, tanto el riesgo¹⁰¹ como, en consecuencia, la citada clasificación, se encuentran íntimamente relacionados con algunas cuestiones muy relevantes y sobre las que se debe discernir, como son la tipología de responsabilidad aplicable (objetiva, *quasi* objetiva o mixta) y la exigencia de un seguro obligatorio. Sobre el particular, hemos de realizar varias observaciones.

En primer lugar, desde nuestra perspectiva, para llevar a cabo la citada clasificación entendemos que han de manejarse diferen-

¹⁰¹ En esta línea destaca ZURITA MARTÍN, I.: *La responsabilidad*, cit., pp. 66-78, que la aplicación de un sistema de responsabilidad objetiva podría repercutir negativamente en la innovación tecnológica. Por ello, propone un sistema de gestión de riesgos que tenga en cuenta tanto el principio de precaución como la determinación del «riesgo aceptable». A este respecto, indica ERCILLA GARCÍA, J.: *Normas de Derecho*, cit., p. 89 que la gestión de riesgos «consiste en identificar analizar y evaluar los riesgos potenciales que podrían poner en peligro dañoso a bienes jurídicos susceptibles de protección».

tes criterios. De un lado, es muy relevante el ámbito en el cual el robot se vaya a utilizar; esto es, en definitiva, los sujetos u objetos con los que se relacione. En este punto, también debemos atender tanto al uso que al que se vaya a destinar el recurso que emplee como al número de personas a las que, en su caso, pueda afectar. Si se repara con detenimiento, lo que se valora es el tipo de daño (personal, material, moral, etc.) y la intensidad del impacto que puede producirse. Como rápidamente se comprenderá, el tratamiento que ha de recibir una máquina cuyo objetivo sea intervenir en el sector sanitario no será equivalente a aquella otra que únicamente trate con datos no personales. En última instancia, se trata del riesgo potencial de daño que un robot inteligente genere, ya que, en función de este último, se recurrirá a un régimen u otro. No obstante, estos riesgos han de ser reales y estar basados en lo empírico, no bastando meras lucubraciones o hipótesis infundadas.

Por todo ello, a nuestro parecer, la precitada clasificación se ha de elaborar con base en criterios fiables y contrastados y que, en última instancia, encuentren su fundamento en argumentos probabilísticos de causación de perjuicios. Los sistemas de inteligencia artificial se deben catalogar en función del riesgo real y efectivo que generen y en atención a ciertas reglas como la actuación en vías públicas, el contacto con personas y, en su caso, el número de posibles afectados, el tipo de datos que maneje o la relevancia de los derechos que pueda conculcar.

En segundo lugar, en la línea de lo que hemos mantenido anteriormente, entendemos que se ha de evitar atender a la autonomía o automatización de las máquinas en este ámbito. En contra, el Considerando 13 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial alude al grado de autonomía en la toma de decisiones para clasificar los sistemas. En esta línea, el artículo 3 c) de la citada norma, al definir el alto riesgo, destaca que la magnitud del potencial depende, entre otras cosas, del mencionado grado de autonomía de la toma de

decisiones. Como regla general, pues, podemos señalar que, a mayor presencia de una persona, menor riesgo existirá de generar daño¹⁰² y, al contrario, si disminuye este control y el robot actúa de forma independiente, aumentará el mismo.

No obstante, consideramos que esta conclusión viene amparada en varias hipótesis erróneas. Por un lado, no es cierto que un sistema de inteligencia artificial pueda actuar de forma totalmente independiente. Los mismos siempre precisarán de la intervención de un humano que le permita “aprender” y “entrenar”. Además, tampoco hemos alcanzado, en la actualidad, el mayor grado de automatización de tareas, que supondría la forma más elevada de autonomía. Por otro lado, no es adecuado interpretar que, el grado de libertad con el que opera el robot y, por tanto, la menor intervención del humano conlleva, *per se*, un mayor riesgo. Este razonamiento integra en, al menos, dos presupuestos des-
acertados o, si se quiere, incurre en dos falacias.

Así, partiendo de la que podemos denominar «falacia tecnológica¹⁰³», se viene considerando por parte de algunos autores que la implementación de la tecnología implica que la máquina posee, como mínimo, los mismos sesgos¹⁰⁴, convicciones y errores

¹⁰² A este respecto, las Directrices éticas para la inteligencia artificial elaboradas por el grupo de expertos a las que hacíamos referenciar anteriormente, señalan que «La supervisión humana ayuda a garantizar que un sistema de IA no socave la autonomía humana o provoque otros efectos adversos». Por este motivo, entiende el grupo de expertos que, si el resto de las circunstancias no cambian, «cuanto menor sea el nivel de supervisión que pueda ejercer una persona sobre un sistema de IA, mayores y más exigentes serán las verificaciones y la gobernanza necesarias».

¹⁰³ Este término es empleado, en un sentido diferente al propuesto, en KANE, G.C./PHILLIPS, A.N./COPULSKY, J.R.: *The Technology Fallacy: How People Are the Real Key to Digital Transformation*, Massachusetts, MIT Press, 2019.

¹⁰⁴ Acerca de la responsabilidad civil por los sesgos discriminatorios, *vid.* GONZÁLEZ VALVERDE, A.: «Responsabilidad por el potencial sesgo discriminatorio de los algoritmos de los productos de Inteligencia Artificial. A propósito de la *Algorithmic Accountability Act of 2019 (s.1108)*», en *Cuestiones clásicas y actuales*

que la persona que, en definitiva, la crea. Sin embargo, no existe una certeza científica para aseverar una conclusión semejante. Muy al contrario, tal y como antes señalamos, la propia razón que empuja a desarrollar la inteligencia artificial es que pretende mejorar el rendimiento obtenido en un determinado campo.

En todo caso, si bien la anterior reflexión puede ser acertada en la actualidad, no lo será para la tecnología que se desarrolle en un futuro próximo. A este respecto, uno de los rasgos característicos de dicha inteligencia es que la misma puede entrenar y aprender de forma continua, de tal forma que los resultados serán, cada vez, más cercanos a lo óptimo.

Igualmente, incorpora la «falacia de la racionalidad del ser humano», pues entiende que cuando existe una persona que actúa acompañando o revisando al sistema se reduce la posibilidad de que se genere un daño. En suma, parte de la idea de que el humano, siempre y en todos los casos, procede de una forma racional, lógica y razonable. De hecho, este posicionamiento ha sido acogido en la reciente Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas de inteligencia artificial (*artificial intelligence act*). En este sentido, en su artículo 14 requiere que los sistemas de alto riesgo sean supervisados por una persona, de tal forma que tal intervención tendrá como objetivo prevenir o minimizar los riesgos para la salud, la seguridad o los derechos fundamentales.

No obstante, la experiencia nos demuestra que este extremo no es real y que, incluso, sucede en un sentido contrario. Tanto es así, que algunos estudios afirman que la interacción «del ser humano con los artefactos, y muy especialmente con los sistemas complejos no es fácil», y que, además, «se estima que el error humano es la causa primaria del 60-70% de los acciden-

tes e incidentes que tienen lugar en estos sistemas complejos¹⁰⁵». En definitiva, esta interacción tampoco asegura, desde ningún punto, la ausencia de riesgo. Las personas pueden cometer, al menos, los mismos errores que un robot inteligente. Asimismo, no nos parece adecuado entender que una máquina es peligrosa y apta para generar daños. Muy al contrario, su aplicación facilita la vida en sociedad y permite alcanzar beneficios que, de otro modo, no sería posible.

En tercer lugar, sería interesante que la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial incorporara una distinción entre los sistemas que únicamente operen en el contexto cibernético y otras que, por el contrario, tengan presencia en el mundo físico. Como rápidamente se comprenderá, los potenciales daños que se derivan en uno u otro supuesto varían notablemente y han de ser tenidos en cuenta por el legislador. Precisamente este motivo es el que refuerza la conclusión a la que llegaremos posteriormente relativa a la necesidad de que, en determinados casos, se aprueben normativas específicas. Todo ello, muestra las diversas aplicaciones de esta tecnología y, por tanto, los múltiples ámbitos en los que puede implementarse. No obstante, existen marcadas diferencias entre cada una, pues presentan particularidades que han de ser atendidas.

En cuarto lugar, a la hora de valorar los daños que se pueden producir, consideramos que merecen especial mención aquellos colectivos que puedan ser considerados especialmente vulnerables (como menores de edad, mayores dependientes, personas con discapacidad¹⁰⁶, etc.). Asimismo, se debería llevar a cabo un

¹⁰⁵ En este sentido, *vid.* SEBASTIÁN CÁRDENAS, M.L.: «Fallo humano: la quiebra de un paradigma», *Apuntes de Psicología*, vol. 27, núm. 1, 2009, p. 22; WICKENS, C.D.: *Engineering psychology and human performans*. Nueva York, Harper Collins, 1992.

¹⁰⁶ A este respecto, destaca la citada Resolución de 20 de octubre de 2020 sobre los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, en su Considerando 38, que «la inteligencia artificial, la robótica y las

estudio exhaustivo acerca de los efectos negativos que sobre las máquinas puedan tener sus aplicaciones (por ejemplo, decisiones sesgadas¹⁰⁷, discriminación¹⁰⁸, etc.) y establecer propuestas para minimizar los mismos. En este sentido, adquieren importancia la tutela de los derechos fundamentales (como la intimidad¹⁰⁹, la integridad física y moral, la igualdad, la libertad religiosa o la dignidad), la protección de datos y de los consumidores y usuarios, la propiedad intelectual e industrial, entre otros. Como se observa, todo lo anterior engloba a la responsabilidad civil en su totalidad, esto es, los ámbitos contractual y extracontractual.

En quinto lugar, nos gustaría reflexionar acerca de una exclusión de la aplicación de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. En este sentido, el artículo 3 letra h) de la misma define «persona afectada»:

tecnología conexas socialmente responsables tienen un papel que desempeñar en la búsqueda de soluciones que salvaguarden y promuevan los valores fundamentales de nuestra sociedad, como la democracia, el Estado de Derecho, la pluralidad e independencia de los medios de comunicación y una información objetiva y de libre acceso, la salud y la prosperidad económica, la igualdad de oportunidades, los derechos sociales y laborales de los trabajadores, una educación de calidad, la protección de la infancia, la diversidad cultural y lingüística, la paridad de género, la alfabetización digital, la innovación y la creatividad; recuerda la necesidad de velar por que los intereses de todos los ciudadanos, incluidos los que están marginados o en situación de vulnerabilidad, como las personas con discapacidad, sean tenidos en cuenta y estén representados debidamente».

¹⁰⁷ En este sentido, *vid.* el artículo 9 de la Propuesta de Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas.

¹⁰⁸ Sobre el particular, *vid.* el artículo 10 sobre responsabilidad social e igualdad de género de la Propuesta de Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas.

¹⁰⁹ *Vid.* artículo 12 de la Propuesta de Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas que regula el respeto de la intimidad y protección de los datos personales.

tada» como «toda persona que sufre daños o perjuicios por una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA, y que no sea su operador». Precisamente esta referencia relativa al «operador» es la que impide que, si este sujeto sufre un daño, pueda acogerse a la disposición comentada. Surge la duda de la legislación que, en tal situación, ha de aplicarse para resolver la responsabilidad. Máxime cuando el que cause el perjuicio sea también «operador». Imagínese, por ejemplo, que una actuación del operador inicial provoca que el sistema cause un daño al operador final. Nos encontramos, de nuevo, ante una pésima regulación y ante una gran inseguridad jurídica.

En sexto y último lugar, hemos de anudar una idea a lo anterior. A este respecto, como se ha señalado, se debería distinguir entre los casos en los que interactúan máquinas y aquellos otros en los que interviene un ser humano. En este momento, interesa poner de relieve que, en este contexto, podríamos encontrarnos ante una mayor problemática por cuanto las personas somos impredecibles. Sea como fuere, para comprender la realidad (máxime cuando la misma es compleja) llevamos a cabo simplificaciones de la misma, en definitiva, representaciones de lo que entendemos. Por este motivo, en la práctica, siempre que se produzca un daño, el ejercicio se resumirá en depurar la responsabilidad de algunos (o todos) los sujetos intervinientes. En este campo, básicamente, ello se resume en dos grupos de situaciones. De un lado, las que una persona decide separarse de la solución aportada por la máquina. De otro lado, las que siguiendo las directrices marcadas por el sistema, se produce un perjuicio.

De esta suerte, en las primeras se responsabilizará, precisamente, al sujeto que, unilateralmente, estima que no es adecuado cumplir con las indicaciones. Por su parte, en las segundas se buscará el error y, por tanto, la persona que se equivocó. En todo caso, de no ser posible lo anterior, como veremos, regirá la solidaridad (art. 11 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial).

3.4. Los criterios de responsabilidad incluidos en la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial

En este momento, una vez que hemos determinado el ámbito de aplicación de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial y, por tanto, los sujetos que pueden ser declarados responsables a su amparo, conviene que nos centremos en las reglas que maneja esta norma para determinar dicha responsabilidad. Esto último conlleva que tengamos que estudiar, al menos, los criterios de imputación, las causas eximentes, las clases de daños indemnizables y sus límites y el plazo de prescripción previsto. Como se tendrá ocasión de comprobar, las diferencias con respecto a otras normas (Directiva de responsabilidad por productos defectuosos o leyes nacionales de responsabilidad) son notables y, por ello, merece un análisis pormenorizado. Sea como fuere, es interesante que en cada uno de los ámbitos repasemos, con carácter previo y de forma muy resumida, la evolución experimentada en el seno de la Unión Europea con la finalidad de, en última instancia, concretar la solución que ha sido acogida.

3.4.1. Criterios de imputación

Sobre el particular, entendió la Resolución del Parlamento Europeo, de 16 de febrero de 2017, que lo idóneo era la determinación de una responsabilidad objetiva, en la cual se tendría que probar únicamente el nexo causal entre el funcionamiento perjudicial del robot y los daños causados a la persona. Sin embargo, se permitía que el fabricante, el programador, el propietario o el usuario pudieran beneficiarse de un régimen de responsabilidad limitada si contribuían a un fondo de compensación o bien si suscribían conjuntamente un seguro que garantizase la compensación de daños o perjuicios causados por un robot.

Por su parte, el Informe del grupo de expertos matizó estas cuestiones. Así, en cuanto a la causalidad, señaló que era posible que se recurriera a una inversión de la carga probatoria¹¹⁰ en ciertas circunstancias tales como: la probabilidad de que dicha tecnología contribuyese al daño, el riesgo de un defecto conocido dentro de la misma (a pesar de que su impacto causal no sea evidente), el grado de inteligibilidad de los procesos que pueden haber contribuido a la causa o el incumplimiento de las normas de seguridad. En el ámbito de la culpabilidad, partió de una responsabilidad subjetiva, a pesar de que indicó que, en realidad, muchas de las disposiciones aplicables incluyen un régimen de responsabilidad objetiva. Sea como fuere, no parece que siempre tengamos que recurrir a esta clase de responsabilidad, debiendo ser los distintos estados los que determinen la concreción de esta dualidad de sistemas. De hecho, incluso para determinar la responsabilidad del productor o del operador (que es, en principio, objetiva), se destacó que también es posible exigir la misma por la inobservancia de los deberes de cuidado.

Por otro lado, el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la

¹¹⁰ A este respecto, parte de la doctrina señala que los sistemas de inteligencia artificial pueden contar con capacidad para guardar información relevante y que, en su caso, sea utilizada por las víctimas. Esto último no conlleva, como es lógico, el acceso al algoritmo que incorpora la tecnología en cuestión, ya que podría dar lugar a situaciones poco deseables. Para lograr este extremo, se tendría que favorecer la transparencia de las compañías con medidas previstas en el ordenamiento e, incluso, a partir de incentivos judiciales (a la hora de valorar la culpa). Por todo ello, salvo en los casos límite, no tendría que recurrirse a soluciones excepcionales de inversión de la carga probatoria. En este sentido, *vid.* RUBÍ PUIG, A.: «Retos de la inteligencia», *cit.*, p. 63; HACKER, P./KRESTEL, R./GRUNDMANN, S./NAUMANN, F.: «Explainable AI under contract and tort law: legal incentives and technical challenges», *Artificial Intelligence and Law*, vol. 28, 2020, pp. 415-439.

robótica, de 19 de febrero de 2020, para adaptar las normativas nacionales, prevé que «la carga de la prueba podría vincularse al cumplimiento (por el agente pertinente) de obligaciones específicas en materia de ciberseguridad u otras obligaciones en materia de seguridad establecidas por ley: si no cumple estas normas, podría modificarse la carga de la prueba por lo que se refiere a la culpa y la causalidad». Además, en aplicaciones con un perfil de riesgo específico, se comenzó a recabar opiniones acerca del establecimiento de una responsabilidad objetiva y su vinculación con un seguro. Por su parte, «en relación con el funcionamiento de las demás aplicaciones de la inteligencia artificial, que son la gran mayoría, la Comisión está reflexionando sobre si procede adaptar la carga de la prueba relativa a la causalidad y la culpa».

Pues bien, finalmente la Resolución de 20 de octubre de 2020 sobre responsabilidad civil ha destacado que, normalmente, no existirá vínculo contractual con las víctimas y que, por ello, únicamente dispondrían de la responsabilidad subjetiva del Derecho de daños «y podrían tener dificultades para demostrar la culpa del operador del sistema de IA, por lo que podrían fracasar las correspondientes demandas por responsabilidad civil». Además, en el caso de concurrir varios operadores, todos han de ser responsables civiles solidarios (artículo 11 del Reglamento propuesto¹¹¹). No obstante lo anterior, tal y como tuvimos ocasión de señalar, al igual que el Informe de la Comisión al Parlamento Europeo,

¹¹¹ Asimismo, el artículo 12.2 del Reglamento propuesto prevé la posibilidad de vía de regreso en aquellos casos en los que uno de los operadores que resulte responsable solidario haya abonado la totalidad de la indemnización. A este respecto, señala que los porcentajes de responsabilidad se basarán en los respectivos niveles de control por parte de los operadores sobre el riesgo relacionado con la operación y el funcionamiento del sistema de inteligencia artificial. Igualmente, el apartado tercero del citado artículo regula la posibilidad de que el operador ejercita una acción de resarcimiento frente al productor del sistema de inteligencia artificial defectuoso de conformidad con la Directiva 85/374/CEE y las disposiciones nacionales en materia de responsabilidad por los daños causados por productos defectuosos.

al Consejo y al Comité Económico y Social Europeo de 19 de febrero de 2020, considera que el riesgo predicable de los distintos sistemas de inteligencia artificial no es equivalente.

Así, propone un régimen basado en este extremo que deberá regularse de forma exhaustiva. Como vimos, diferencia entre los sistemas de alto riesgo (a los que incorpora una responsabilidad objetiva y la exigencia de un seguro) y los aquellos que no dispongan de tal carácter (que quedarán sujetos a la responsabilidad subjetiva pero con una inversión del *onus probandi*). Por su parte, por lo que respecta a los sistemas de inteligencia artificial que no hayan sido evaluados por la Comisión y que no estén clasificados, se regirán por la responsabilidad objetiva si han causado incidentes reiterados que den lugar a un daño o un perjuicio grave.

3.4.2. *Causas eximentes, tipos de daños indemnizables, límites y plazo de prescripción: la posible aplicación del estado de la ciencia*

Tal y como hemos tenido ocasión de señalar, los sistemas de inteligencia artificial han de ser clasificados en función del riesgo que generen, por lo que debemos referirnos de forma separada a cada uno de ellos. En primer lugar, para aquellos que sean considerados de alto riesgo, hemos señalado que la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial prevé una suerte de responsabilidad objetiva y la obligatoriedad de suscripción de un seguro. Debido a este carácter, en principio, las únicas causas eximentes de la responsabilidad aplicables a este campo serían la fuerza mayor o la culpa exclusiva de la víctima. En este sentido, el artículo 10.1 de la citada norma señala que «Si el daño o perjuicio es causado por una actividad física o virtual, un dispositivo o un proceso gobernados por un sistema de IA o por la actuación de una persona afectada o de una persona de la que la persona afectada sea responsable, el alcance de la responsabilidad civil del operador con arreglo al pre-

sente Reglamento se reducirá en consecuencia. El operador no será responsable si la persona afectada o la persona de la que esta es responsable es la única a la que se le puede achacar el daño o perjuicio causado». Podemos, pues, encontrarnos ante una concurrencia de culpas e, incluso, ante una exención total de responsabilidad¹¹².

De hecho, el apartado segundo del mismo artículo destaca que cuando el operador sea considerado responsable, podrá utilizar los datos generados por el sistema de inteligencia artificial para demostrar la negligencia concurrente de la persona afectada respetando, en todo caso, las exigencias previstas en el Reglamento (UE) 2016/679 y otras leyes en materia de protección de datos relevantes. Asimismo, también la persona afectada también podrá usar esos datos con fines probatorios o aclaratorios en la demanda por responsabilidad civil.

Por su parte, no prevé las consecuencias de la posible intervención de un tercero. De hecho, tanto el Considerando 9 de la Resolución de 20 de octubre de 2020 sobre responsabilidad civil (que reproduce de forma similar el propio Considerando 9 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial) excluyen de su ámbito de aplicación «los perjuicios causados por un tercero interferidor como un pirata informático», al entender que esta interferencia, por regla gene-

¹¹² A este respecto, ERCILLA GARCÍA, J.: *Normas de Derecho*, cit., p. 87 destaca que «al tratarse de un sistema de responsabilidad objetiva, la carga de la prueba de la exculpación, ex art. 27 ILEC, habrá de recaer sobre los Agentes Intervinientes que habrán de acreditar que el proceder dañoso del robot, no fue debido a un error de programación de su inteligencia artificial (*culpa in codificando*), o a un fallo de fabricación de sus elementos físicos (*culpa in faciendo*), o a una formación en fase de aprendizaje supervisado incorrecta (*culpa in educando*), o de una falta de mantenimiento de los sensores del robot (*culpa in curando*), sino que en todo caso se trataría de culpa exclusiva de la víctima o de fuerza mayor». No obstante, como señala el autor citado, el problema se plantea, igualmente, en los casos de acción autónoma del robot (*culpa in singularitatem*), que sería un caso fortuito pero no excluyente de responsabilidad.

ral, constituye una acción de responsabilidad civil subjetiva y «la legislación vigente de los Estados miembros en materia de responsabilidad subjetiva ofrece, en la mayoría de los casos, un nivel de protección suficiente». Únicamente en aquellos casos en los que ese tercero no sea rastreable o sea insolvente «parece necesario añadir normas en materia de responsabilidad civil para complementar la legislación nacional en materia de responsabilidad civil existente». No obstante, en estos últimos supuestos, tampoco concreta a qué disposiciones debemos acudir ni si, en suma, es aplicable la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial.

Desde nuestra perspectiva, entendemos que sí cabe recurrir a esta norma siempre que ese tercero pueda ser considerado como operador y no exista otra legislación especial. Siguiendo con el principio de resarcimiento integral de la víctima no resulta adecuado que, de forma injustificada, se niegue dicha compensación por el mero hecho de que sea otro sujeto quien cause el daño.

En otro orden de cosas, al igual que en la Directiva sobre responsabilidad por productos defectuosos, la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial analizada impide que se acuerde una limitación o exención de responsabilidad en este campo, debiendo ser considerado tal extremo, de producirse, como nulo de pleno derecho (art. 2.2 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial).

Por otro lado, en cuanto a los tipos de perjuicios que cabe reparar en este sector, hay que tener en cuenta que cabe tanto anudar los menoscabos de tipo personal como los que afecten a bienes materiales. En el primer grupo, podremos encontrarnos supuestos de fallecimiento¹¹³ o de afectación de la salud o la inte-

¹¹³ A este respecto, señala el artículo 6.1 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial que, dentro de los límites indemnizatorios previstos en el artículo 5.1 letra a), «la indemniza-

gridad física¹¹⁴, así como de daños morales. En este último caso, señala la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial que han de traducirse en una pérdida económica comprobable, por lo que no es posible solicitar, en principio, cualquier clase de daño. Asimismo, el artículo 5 de la citada Propuesta de Reglamento recoge un importe máximo indemnizatorio en función del detrimento producido. Cuando nos encontremos ante casos de fallecimiento o de perjuicio en la salud o la integridad física dicha cantidad es de dos millones de euros.

ción que abonará el operador considerado responsable en caso de daños físicos seguidos de la muerte de la persona afectada se calculará sobre la base de los costes del tratamiento médico que haya seguido la persona afectada antes de su muerte, así como del perjuicio económico sufrido antes del fallecimiento como consecuencia del cese o la reducción de la capacidad de generar ingresos o el aumento de sus necesidades mientras durase el daño antes del fallecimiento. El operador será además responsable de reembolsar los gastos funerarios de la persona afectada fallecida a la parte responsable de sufragar dichos gastos».

Además, destaca el párrafo segundo del citado precepto que «Si en el momento del incidente que causó el daño que condujo a su muerte, la persona afectada mantenía una relación con un tercero y tenía la obligación jurídica de asistir a ese tercero, el operador responsable indemnizará al tercero mediante el pago de una pensión alimenticia proporcional a la que la persona afectada se habría visto obligada a pagar, durante un período equivalente a la esperanza de vida media de una persona de su edad y teniendo en cuenta su estado general. El operador también indemnizará al tercero si, en el momento del incidente que provocó la muerte, el tercero había sido concebido, pero todavía no había nacido».

¹¹⁴ En este sentido, el artículo el artículo 6.2 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial que, dentro de los límites indemnizatorios previstos en el artículo 5.1 letra b), «la indemnización que pagará el operador considerado responsable en caso de daño para la salud o para la integridad física de la persona afectada incluirá el reembolso de los gastos del tratamiento médico correspondiente, así como el pago del perjuicio económico sufrido por la persona afectada como consecuencia de la suspensión temporal, la reducción o el cese definitivo de su capacidad de generar ingresos o del aumento consiguiente de sus necesidades acreditado mediante certificado médico».

Por su parte, si se trata de daños morales o a los bienes, la suma es de un millón de euros. Sin embargo, indica la referida norma que cuando nos movamos ante esta clase de lesiones y la persona afectada también disponga de un derecho a reclamar por responsabilidad contractual contra el operador «no se abonará ninguna indemnización en virtud del presente Reglamento si el importe total de los perjuicios materiales o el daño moral es de un valor inferior a 500 euros».

Sea como fuere, si la indemnización ha de abonarse a varias personas que sufran daños o perjuicios causados por el mismo funcionamiento de un sistema de inteligencia artificial y el importe total supere los límites antes referidos, prevé la señalada Propuesta de Reglamento que la cantidad que deba entregarse a cada persona se reducirá proporcionalmente «de forma que la indemnización combinada no supere los importes máximos establecidos». Repárese, no obstante, que se alude a que la lesión sea consecuencia de un funcionamiento concreto del sistema, por lo que no resultará de aplicación este extremo cuando dichos daños se produzcan por distintas actuaciones del mismo. Imagínese que, por ejemplo, que un robot que se emplea en el ámbito sanitario ofrece un diagnóstico errado a un paciente y, por otro lado, sufre una “fuga de información” que afecta a otro usuario distinto. En este escenario, no parece que deba recurrirse a la reducción proporcional a la que antes hacíamos referencia, ya que se trata de dos funciones distintas y separadas.

Por lo que se refiere al plazo de prescripción, destaca el artículo 7.1 del Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial que cuando se trate de daños a la vida, la salud o la integridad física estarán sujetas a un plazo de prescripción especial de treinta años. En otro orden de cosas, si nos encontramos ante perjuicios materiales o morales, el artículo 7.2 de la misma norma establece dos plazos, de los cuales será aplicable el que venza antes. Por un lado, se recoge el de diez años a partir de la fecha en que se produjo el menoscabo a los bienes o la

pérdida económica comprobable resultante del daño moral significativo, respectivamente y, por otro, el de treinta años a partir de la fecha en que tuvo lugar la operación del sistema de inteligencia artificial de alto riesgo que causó posteriormente el menoscabo a los bienes o el daño moral.

En segundo lugar, aquellos sistemas que no merezcan la consideración de alto riesgo, a la ausencia de exigencia de un seguro obligatorio, debemos añadir el establecimiento de una responsabilidad subjetiva, esto es, que atiende a la culpa (artículo 8.1 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial). Sin embargo, si deparamos con detenimiento en la regulación, podemos concluir que, en realidad, estamos ante una responsabilidad cuasiobjetiva, ya que se aplica una suerte de inversión de la carga probatoria. Desde esta perspectiva, será el demandado (operador) quien tendrá que demostrar que actuó con la diligencia debida. En este campo, esta prueba se concreta en la acreditación de los extremos contemplado en el apartado segundo del mencionado artículo, a saber:

- Que el sistema se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador.
- O que se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de inteligencia artificial adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de inteligencia artificial, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles.

En este sentido, se opta por el establecimiento de un estándar de conducta basado en una serie de presunciones *iuris tantum*. De algún modo, con este extremo se objetiva el contenido de la *lex ar-*

tis aplicable a este ámbito. De hecho, esta línea ya venía recogida en otros textos anteriores como el Informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies». No obstante, en la citada Propuesta de Reglamento se anudan una serie de criterios que difieren de otros que también podrían resultar relevantes tales como el cumplimiento de medidas o normas de actuación¹¹⁵, la suscripción de determinadas garantías, la inscripción en registros públicos o la adhesión a códigos éticos y de conducta.

Por otro lado, en cuanto a las causas eximentes de responsabilidad, interesa señalar que son aplicables las que anteriormente analizamos en el ámbito de los sistemas de alto riesgo. Desde esta perspectiva, el ya citado artículo 8.2 de la Propuesta de Reglamento mencionada, *in fine*, prevé que el operador no será responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. Además, en este caso sí se hace mención expresa a la intervención de un tercero interferidor. Así, el apartado tercero del mencionado artículo indica que «Cuando el daño o perjuicio haya sido causado por un tercero que haya interferido en el sistema de IA por medio de una modificación de su funcionamiento o sus efectos, el operador será, no obstante, responsable del pago de una indemnización en caso de que dicho tercero esté ilocalizable o sea insolvente». De esta suerte, cuando ese tercero se encuentre localizado y no sea insolvente estaremos ante una exención de responsabilidad en favor del operador.

Igualmente, hemos de traer a colación las reflexiones que llevamos a cabo sobre los tipos de daños indemnizables. A pesar de que no se refiera este extremo, parece que tienen vigencia las mismas consideraciones que para los de alto riesgo. No cabe predicar

¹¹⁵ En este sentido, el Libro Blanco sobre la inteligencia artificial antes comentado establece una distinción entre aplicaciones de inteligencia artificial consideradas de riesgo elevado y aquellas que no lo son. Así, como vimos, impone una serie de requisitos legales obligatorios para las primeras y propone, para las segundas, un sistema de etiquetado voluntario.

algo similar, sin embargo, con respecto al plazo de prescripción, a los importes y al alcance de la indemnización, ya que el artículo 9 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial lo excluye expresamente al señalar que las demandas estarán sujetas a la legislación del Estado miembro en el que se haya producido el daño o perjuicio. Se aplica, pues, la regla del *forum loci delicti comissi* y, para dilucidar estos aspectos, tendremos que atender al ordenamiento jurídico nacional que corresponda.

En tercer y último lugar, hemos de referirnos a los sistemas de inteligencia artificial que no hayan sido evaluados por la Comisión y que no estén clasificados. A este respecto, el Considerando 20 de la Resolución de 20 de octubre de 2020 sobre responsabilidad civil prevé que cuando tales sistemas produzcan un perjuicio, como regla general, han de quedar sujetos a la responsabilidad subjetiva. No obstante, matiza esta cuestión en dos sentidos. De un lado, porque al igual que para los sistemas que no sean considerados de alto riesgo, es aplicable la inversión de la carga probatoria (o, si se quiere, la presunción de culpa del operador). De otro lado, porque el Considerando 21 de la misma norma señala que, excepcionalmente, cuando cause incidentes reiterados que den lugar a un daño grave, tendremos que recurrir a la responsabilidad objetiva. En este escenario, «la Comisión también debe evaluar, sin demora indebida, la necesidad de revisar dicho anexo para añadir el sistema de IA en cuestión a la lista» y si, a raíz de dicha evaluación, «la Comisión decide incluir dicho sistema de IA en la lista, dicha inclusión debe tener efecto retroactivo a partir del momento del primer incidente probado causado por dicho sistema que haya ocasionado un daño o un perjuicio grave».

Por su parte, el Considerando 22 de la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial incide en la importancia de que se creen fondos especiales de indemnización para cubrir estos casos. Para que esto último funcione correctamente y para transmitir seguridad jurídica,

indica que tanto la existencia de dicho fondo como las condiciones para acogerse a él, deben hacerse públicas de manera clara y exhaustiva.

Tras ello, cabe plantearse qué hemos de entender por perjuicio grave, ya que la citada Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial no incluye ninguna pauta. Únicamente disponemos del Considerando 3 de la mencionada norma, en el que se prevé que estos daños se producen, por ejemplo, cuando se ponga en peligro «la dignidad humana y los valores y libertades europeos mediante el seguimiento de las personas contra su voluntad, la introducción de sistemas de crédito social o la toma de decisiones sesgadas en materia de seguro de enfermedad, concesión de crédito, autos judiciales, contratación o empleo o mediante la construcción de sistemas armamentísticos autónomos letales». Sería recomendable, por tanto, que en el futuro Reglamento se tuviera en cuenta este extremo y se regulase de forma detallada. De otro modo, nos encontramos ante una situación de inseguridad jurídica que, además, puede desembocar en una diferencia de trato injustificada.

En otro orden de cosas, hemos de reflexionar sobre el papel que ocupa el estado de la ciencia¹¹⁶ en este ámbito. Este último

¹¹⁶ En este sentido, señala DE LAS HERAS GARCÍA, Manuel Ángel, «*Lex Artis, Onus Probandi* y responsabilidad médica», *Revista jurídica de la Región de Murcia*, núm. 36, 2005, pp. 17-19 que «Bajo la amplia fórmula *lex artis* (*leges artium, legis artis* o reglas del arte, entre otra terminología) se engloba el contenido de la libre y diligente actuación profesional, esto es, abriga aquella serie de actitudes y conocimientos aplicables a su ejercicio cuya obtención y práctica conlleva que el profesional sea socialmente reconocido como tal. A pesar de que esta propia voz -profesional- constituye un noción metajurídica, con varias significaciones, arrancando del sentido gramatical de profesión y en su acepción eminentemente sociológica equivale a ostentar determinados conocimientos en una concreta materia que llevan aparejados una cualificación profesional (plasmada, a su vez, en una certificación o título), constituyendo lo más característico de las profesiones liberales -como es la médica- la autonomía o independencia en su ejercicio con sometimiento, como criterio rector, a esta denominada *lex artis* con carácter

aparece como el nivel de conocimientos científicos y técnicos existentes en un determinado momento, ya que los hechos han de valorarse atendiendo a las posibilidades reales que tenía el sujeto actuante. Así, podemos traer a colación lo ocurrido en supuestos en los que, debido al conocimiento del momento, no se imputaron los daños al demandado. Por ejemplo, por su repercusión, cabe citar el caso de los contagios producidos por VHC (hepatitis C). A este respecto, la doctrina aludió a estas disquisiciones, señalando que «la comunidad científica internacional conocía, desde 1975, la existencia de un virus causante de la hepatitis que no era ni A ni B, así como lo es que no fue hasta 1989 cuando pudo identificarse el virus de la hepatitis C (VHC) y, por consiguiente, pudo desarrollarse el primer test de detección del virus en cuestión. También es cierto que en el Estado español, la obligación de analizar la presencia de VHC en las donaciones de sangre se impuso en octubre de 1990¹¹⁷». Igualmente, la jurisprudencia se manifestó en estos términos¹¹⁸.

prácticamente exclusivo. Diversos han sido los conatos en orden a definir esta *lex* (identificada, por lo general, con aquella regla de la técnica de actuación de la profesión que se trate) la cual viene referida, en último término, a aquella esfera de autonomía profesional cuya regulación exclusivamente incumbe a sus miembros (reputados artífices o profesionales) que, a la postre, son los encargados de encarnar un modelo de conducta representado por las reglas o técnicas específicas de un concreto arte u oficio incumbiendo, por ende, el establecimiento de tal *lex* en Medicina a la propia profesión médica. Cabe mantener que las *leges artium* de cada profesión son aquéllas que gobiernan la actuación de los profesionales que consideremos, toda vez que el genérico modelo de conducta del buen padre de familia se caracteriza, precisamente, por la negación de todo conocimiento técnico, su naturaleza no profesional o especializada».

¹¹⁷ En este sentido, *vid.* BLAS ORBÁN, C.: «Contagio transfusional de VHC. Reflexiones sobre la previsibilidad del daño», *DS*, vol. 16, núm. 2, 2008, pp. 181-182.

¹¹⁸ *Vid.*, entre otras, las SSTS núm. 9345/1996 Sala Tercera 17 abril 2001 (RJ 4215), núm. 6972/1997 Sala Tercera 1 noviembre 2001 (RJ 10098), núm. 7126/1997 Sala Tercera 22 noviembre 2001 (RJ 20025432), núm. 5446/2005 Sala Tercera 8 octubre 2010 (RJ 7214).

Por su parte, también la transmisión de VIH (virus de la inmunodeficiencia humana) planteó equivalentes problemáticas, sobre lo cual se indicó que «Los avances de la ciencia no han sido paralelos en cuanto a técnicas de control de hemoderivados y de transfusiones sanguíneas, por lo que su tratamiento debe hacerse por separado¹¹⁹». El Tribunal Supremo destacó en diversas sentencias que «hasta el año 1985 el estado de los conocimientos de la técnica no permitía detectar la existencia de VIH en sangre, por lo que todas las transfusiones de plasma, efectuadas con anterioridad a dicho año 1985, en que se hubiera podido inocular el indicado virus, no generan responsabilidad patrimonial de la Administración sanitaria por no ser la lesión causada antijurídica¹²⁰».

De esta forma, en el ámbito de una situación extraordinaria y debido a la ausencia de certezas acerca de la misma es posible que no se pueda responsabilizar de los perjuicios a una persona. Desde esta perspectiva, no cabe, pues, atribuir a un sujeto una consecuencia negativa que, de ningún modo, pudo prever, detectar y modificar. Se trata, en suma, de una exención de responsabilidad que se recoge en algunas normas como la propia Directiva de responsabilidad por productos defectuosos (*vid.* art. 7). No obstante, tal y como reconoce el artículo 15.1 b) de esta última norma, aquellos estados que lo estimen oportuno, podrán «disponer en su legislación que el productor sea responsable incluso si demostrara que, en el momento en que él puso el producto en circulación, el estado de los conocimientos técnicos y científicos no permitía detectar la existencia del defecto». A este respecto, si bien el artículo 140.1 e) contempla este supuesto de exención de responsabilidad, posteriormente, en el apartado tercero del mis-

¹¹⁹ MUGA MUÑOZ, J.L.: «La responsabilidad patrimonial de las administraciones públicas por el contagio de sida», *RAP*, núm. 136, 1995, p. 287.

¹²⁰ *Vid.*, entre otras, las SSTS núm. 12/2002 Sala Tercera 29 noviembre 2002 (RJ 2003\283), núm. 2911/2001 Sala Tercera 10 diciembre 2004 (RJ 2005\473), núm. 172/2005 Sala Tercera 13 junio 2006 (RJ 3469).

mo artículo, excepciona los casos de medicamentos, alimentos o productos alimentarios destinados al consumo humano.

En principio, como en todos los sectores del Derecho de Daños, resulta aplicable este estado de la ciencia. En definitiva, como hemos visto, supone una causa de exoneración que se produce cuando los conocimientos científicos y técnicos existentes no permiten conocer la existencia del defecto o del riesgo. Su aplicación es, en todo caso, restringida a ciertos casos por las especialidades propias de la tecnología implementada. Asimismo, podemos encontrar otra manifestación de este estado de la ciencia cuando el mismo el analizado desde una perspectiva diferente. En este sentido, si una tecnología concreta se muestra como especialmente favorable para remediar o reducir un determinado impacto negativo, podría plantearse si, obligatoriamente, se ha de implementar en el sector de que se trate. A este respecto, lo cierto es que se debería de aplicar un “test” de conveniencia-utilidad y de análisis del nivel de inversión necesario para tratar de concluir lo más adecuado.

Sobre el particular, destaca la doctrina que «el derecho de daños habrá de prever las consecuencias jurídicas de la falta de adopción de una determinada tecnología o de uno de sus estadios de desarrollo. Esto es, habrá de establecer si la falta de adaptación de la tecnología propia a otra más segura resulta siempre negligente o si se permite continuar utilizando una tecnología menos segura sin riesgo de responder civilmente (*grandfathering*). En este examen, también habrá que identificar el nivel de esfuerzos e inversión económica exigibles para superar el umbral que convierta una decisión privada en diligente: por ejemplo, si se obliga únicamente a la adopción del estándar tecnológico común en el sector o se obliga a adoptar la mejor tecnología disponible en términos de seguridad (*Best Available Technology*–BAT¹²¹)». Más tarde volveremos sobre estas cuestiones.

¹²¹ Vid. RUBÍ PUIG, Antoni, «Retos de la inteligencia», *cit.*, pp. 62-63.

Pues bien, el reconocimiento de este extremo lo encontramos en el Informe del grupo de expertos «Liability for Artificial Intelligence and other emerging technologies» que aparece manifestado en los denominados riesgos del desarrollo. Sin embargo, no se recoge de forma expresa en la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial y no se ha incidido en ello. Por este motivo, tenemos que plantearnos si resulta de aplicación o si, por el contrario, esta causa no adquiere vigencia en este sector. Para ofrecer una respuesta hemos de traer a colación la distinción de los sistemas de inteligencia artificial a la que nos hemos venido refiriendo en función del riesgo que entrañan. En este sentido, parece razonable pensar que no podremos recurrir a estas disquisiciones en los de alto riesgo, pues, en definitiva, no atienden a la culpabilidad del sujeto actuante.

No obstante, la conclusión anterior varía si nos centramos en aquellos sistemas que no presentan tal riesgo, ya que, como hemos tenido ocasión de destacar, el criterio de imputación aplicable reside en la negligencia. Algo similar podemos deducir si atendemos al Considerando 18 de la citada Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial, en la que se señala, en la línea de lo que recoge posteriormente el ya mencionado artículo 8.2, que para determinar la diligencia que cabe esperar de un operador ha de tenerse en cuenta que «el operador podría tener un conocimiento limitado de los algoritmos y datos utilizados en el sistema de IA». Por lo tanto, se establecen una serie de presunciones para valorar si, en un caso, el operador ha actuado con la debida atención, a saber: si al seleccionar un sistema de inteligencia artificial ha seleccionado uno que ha sido certificado con arreglo a un sistema similar al sistema de etiquetado voluntario previsto por la Comisión; si durante el funcionamiento del sistema puede demostrar que lo ha supervisado real y periódicamente y ha informado al fabricante sobre posibles irregularidades durante el mismo; si al llevar a cabo el mantenimien-

to de la fiabilidad operativa ha instalado todas las actualizaciones disponibles proporcionadas por el productor.

De alguna forma, con ello se está poniendo de manifiesto que, *a sensu contrario*, si el operador despliega todas aquellas actividades que sean recomendables y necesarias, estaremos ante una actuación diligente. El estado de la ciencia puede impedir que se adopten otras medidas que, *a posteriori*, se presentan como imprescindibles, pero que, *ex ante*, eran desconocidas por la comunidad científica.

Esta interpretación presenta, no obstante, ciertos beneficios e inconvenientes. Sobre los primeros, no podemos obviar que la propia evolución, el desarrollo y el avance de la tecnología implican que se deba actuar sobre entornos no explorados para, precisamente, romper esas barreras. Máxime cuando estamos ante uno de los campos existentes con más nivel de innovación. Por este motivo, establecer un régimen de responsabilidad muy severo podría conllevar que se frenase dicho avance y se impidiese mejorar la vida en sociedad con nuevas implementaciones. Con todo, siendo ello cierto, no podemos perder de vista el hecho de que la finalidad última del Derecho de daños es reparar los perjuicios causados a las víctimas y que, si se interpretase de forma extensiva el estado de la ciencia llegaríamos a situaciones poco deseables en las que estas últimas nunca verían resarcidas sus pretensiones.

Teniendo en cuenta todo lo señalado hasta el momento, consideramos que la solución óptima pasa por ofrecer una respuesta intermedia, que valore las circunstancias *ad casum*. Nos encontramos ante una materia en la que, transversalmente, inciden diversos principios, disciplinas, valores, intereses y derechos, cuya valoración ha de ser tenida en cuenta (en la justa medida). De esta suerte, habrá supuestos en los que los riesgos del desarrollo aconsejen que no se atribuya responsabilidad por un determinado hecho y otros, en los que se entienda que, a pesar del conocimiento limitado, se ha de asumir el riesgo por el operador.

Si se repara con detenimiento, en los primeros casos se está señalando, implícitamente, que las víctimas tienen el deber jurídico de soportar el daño. Nos encontramos, pues, ante un reparto en la asunción de los citados riesgos; en determinadas situaciones deberá llevarlo a cabo el operador y, en otras, la sociedad. En definitiva, la evolución tecnológica y científica conllevan que se asuman ciertos perjuicios ya que, de otro modo, no se permitiría desarrollar e introducir cambios en el sector de que se trate. La cuestión central radica, por tanto, en la determinación del «riesgo razonable o aceptable», esto es, el que ha de ser admitido por la ciudadanía.

Por último, debemos destacar que el artículo 11 de la Propuesta de Reglamento antes referida prevé la solidaridad de la responsabilidad, de tal forma que todos los sujetos que sean potencialmente culpables podrán ser demandados (conjuntamente) y ser condenados en consecuencia (al margen del derecho de repetición reconocido en el artículo 12 de la misma norma).

V.

EL ASEGURAMIENTO DE LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL

En otro orden de cosas, hemos de reflexionar acerca del aseguramiento de la responsabilidad civil derivada de ilícitos producidos como consecuencia de la utilización de la inteligencia artificial. No obstante, conviene tener en cuenta que únicamente se realizará un análisis general y sin atender a los ámbitos concretos en los que se puede manifestar. Sin duda, un estudio completo exigiría estudiar cada uno de estos sectores y sus particularidades para poder concluir, *ad casum*, la solución más adecuada. Sea como fuere, esto último excede de la finalidad de esta obra y no nos detendremos en estas cuestiones. El objetivo pretendido es mucho menos pretencioso, ya que solamente trataremos de determinar unas premisas sobre las que, posteriormente, dilucidar la respuesta más adecuada en atención a las características en el campo de que se trate. De hecho, estas últimas podrán aconsejar que se recurra a un sistema que excepcione, modifique o regule las consecuencias que obtengamos.

A este respecto, como hemos tenido ocasión de comprobar, una de las mayores preocupaciones de la Unión Europea ha sido,

precisamente, el aseguramiento de estas actividades. En este sentido, las instituciones son conscientes del peligro de que las elevadas indemnizaciones desaconsejen a las compañías dedicarse a este sector. Igualmente, la gran inseguridad jurídica existente coadyuva, sin duda, a que estas empresas vean frenadas sus expectativas. A todo ello hay que sumar la incertidumbre en cuanto a los riesgos de los sistemas de inteligencia artificial, ya que son muy variados y es complicado conocer con certeza, *a priori*, la magnitud del daño potencial. Máxime, porque tal y como prevé el artículo 76 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (en adelante, LCS), el afectado dispondrá de una acción directa contra el asegurador (que únicamente podrá oponer la culpa exclusiva de dicho perjudicado o las excepciones personales que tenga contra él).

Por todo ello, nos debemos plantear si el seguro de responsabilidad civil¹²² es suficiente para cubrir los perjuicios derivados del empleo de estas tecnologías o si, por el contrario, es aconsejable recurrir a otros mecanismos (como la suscripción de un seguro específico). Asimismo, como todos los sistemas –o, al menos, la gran mayoría– operan o se sirven de Internet, cobra especial relevancia el ciberseguro o seguro cibernético como una posible modalidad.

Desde nuestra perspectiva, para alcanzar la solución más adecuada es preciso que se establezcan mecanismos que aseguren la participación de las compañías aseguradoras en la aprobación de las distintas normativas. No se puede obviar que, de no ser así, al margen del contenido legal, si las mismas se niegan a suscribir pólizas dicho ámbito quedaría, *de facto*, sin contar con un ase-

¹²² Como hemos tenido ocasión de comprobar, los operadores pueden coincidir o no con los distintos sujetos a los que aludíamos, a saber, productor, fabricante, programador, distribuidor, etc. No obstante, además, señalamos que podría tratarse de un usuario, propietario o poseedor de la máquina que, como regla general, no será un profesional. Desde esta perspectiva, a pesar de que el seguro más habitual en este ámbito sea el referido a la responsabilidad civil empresarial, ello no siempre será así.

guramiento. No obstante, este extremo hay que valorarlo con la correspondiente cautela y de tal idea no se puede concluir, sin embargo, que deba reconocerse una suerte de potestad legislativa en favor de dichas mercantiles. En suma, hemos de recurrir a una ponderación que trate de alcanzar aquella opción que ofrezca cobertura al mayor número de intereses en juego.

1. CONCEPTUALIZACIÓN GENERAL DE LOS SEGUROS DE RESPONSABILIDAD CIVIL: EL RIESGO COMO CRITERIO PARA EXIGIR SU OBLIGATORIEDAD

Como destaca el artículo 73 LCS, el seguro de responsabilidad civil¹²³ es aquel por el que «el asegurador se obliga, dentro de los límites establecidos en la Ley y en el contrato, a cubrir el riesgo del nacimiento a cargo del asegurado de la obligación de indemnizar a un tercero los daños y perjuicios causados por un hecho previsto en el contrato de cuyas consecuencias sea civilmente responsable el asegurado, conforme a derecho».

Sobre el particular, lo cierto es que encontramos diferentes autores¹²⁴ que han tratado de determinar la naturaleza jurídica de

¹²³ En realidad, como pone de relieve la doctrina, este seguro recibe diferentes denominaciones y aplicaciones. En este sentido, MARTÍN OSANTE, J.M.: *El seguro de responsabilidad civil empresarial*, Madrid, Marcial Pons, 2018, p.17, indica que cuando este contrato se circunscribe al ámbito empresarial nos encontramos ante un «contrato de seguro de responsabilidad civil empresarial, también conocido como seguro de responsabilidad civil de explotación de industrias, seguro de responsabilidad civil de explotación de empresas, seguro de responsabilidad civil de industrias, seguro de responsabilidad civil de explotación, seguro de responsabilidad civil por actividades económicas o seguro de responsabilidad civil por actividades económicas empresariales, entre otras denominaciones, constituye una modalidad específica del más genérico contrato de seguro de responsabilidad civil».

¹²⁴ Entre otros, *vid.* LÓPEZ-COBO, C.: *El seguro de responsabilidad civil. Fundamentos y modalidades*, Madrid, Libros Tobal, 1988; PAVELEK ZAMORA, E./

estos contratos, así como las obligaciones que asumen las partes y las implicaciones que conlleva. Máxime por la parquedad del citado precepto en la medida en que no engloba todas las características definitorias del mismo.

En cualquier caso, dejando ello al margen, la primera cuestión a la que hemos de ofrecer una respuesta es la relativa a la obligatoriedad de suscribir un seguro de responsabilidad civil. A este respecto, interesa poner de relieve que no cabe exigir este requisito, con carácter general, para acceder a una determinada actividad. Muy al contrario, el mismo ha de determinarse en atención a la existencia de un riesgo efectivo y a la necesidad, por tanto, de tutelar a las potenciales víctimas¹²⁵. En este sentido, la doctrina científica señala que la regulación del aseguramiento obligatorio de responsabilidad «responde a la necesidad de proteger debidamente a las víctimas, normalmente, de daños ocasionados por actividades potencialmente peligrosas o de riesgo que, si no fuera así, se quedarían sin ser indemnizadas si el responsable no pudiera con su patrimonio hacerse cargo de las indemnizaciones correspondientes¹²⁶».

CAÑIZARES RUBINI, F.: «La responsabilidad civil patronal y su aseguramiento», en *Estudios sobre el aseguramiento de la responsabilidad en la gran empresa* (Dir. F.J. SÁNCHEZ CALERO), Madrid, Musini, SA, 1994, pp. 239-318; PERÁN ORTEGA, J.: *La responsabilidad civil y su seguro*, Madrid, Tecnos, 1998; CALZADA CONDE, M.A.: *El seguro de responsabilidad civil*, Navarra, Aranzadi, 2005; REGLERO CAMPOS, L.F.: «El seguro de responsabilidad civil», en *Tratado de responsabilidad civil* (Coord. L.F. REGLERO CAMPOS/J.M. BUSTO LAGO), 5ª edic., t. I, Navarra, Aranzadi, 2014, pp. 1363-1554; TAPIA HERMIDA, A.J.: «Seguro de responsabilidad civil», en *Estudios sobre el contrato de seguro* (Dir. M.R. QUINTÁNS-EIRAS/L. RAMÍREZ OTERO), Perú, Universidad de Piura, 2017, pp. 599-623.

¹²⁵ En esta misma línea, PAVELEK ZAMORA, E.: «Seguros obligatorios y obligación de asegurarse», *Revista española de seguros: Publicación doctrinal de Derecho y Economía de los Seguros privados*, núm. 106, 2001, p. 241 pone de relieve que el objetivo prioritario de estos seguros es proteger a las víctimas toda vez que se busca un patrimonio solvente que repare los perjuicios causados.

¹²⁶ BADILLO ARIAS, J.A.: «Responsabilidad civil», *cit.*, pp. 54-55.

Sea como fuere, la posibilidad de que los estados miembros puedan integrar estos seguros recibe amparo en diferentes normas. Por su relevancia, cabe destacar la Directiva 2006/123/CE, del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior; la Directiva 2009/138/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II); y la Directiva (UE) 2016/97, del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros. En España, tal regulación viene contenida en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (en adelante, LOSSEAR), que derogó el artículo 75 LCS. De hecho, esta última acoge el precitado riesgo como fundamento de los seguros en su Disposición adicional segunda apartado primero al señalar que «Se podrá exigir a quienes ejerzan determinadas actividades que presenten un riesgo directo y concreto para la salud o para la seguridad de las personas, incluida la seguridad financiera, la suscripción de un seguro u otra garantía equivalente que cubra los daños y perjuicios que puedan provocar y de los que sean responsables».

2. EL ASEGURAMIENTO OBLIGATORIO EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL Y SU COBERTURA

Por un lado, siguiendo el razonamiento anterior, debemos plantear si, en el campo de las máquinas inteligentes existe justificación suficiente para exigir un seguro de este tipo. Sobre el particular, ya destacamos que el análisis ha de estar basado en el riesgo, esto es, el potencial peligro de generar daños. A este respecto, comentando la referida Resolución del Parlamento

Europeo, de 16 de febrero de 2017, destaca BADILLO ARIAS¹²⁷ que «no hay duda de la justificación del seguro obligatorio al que se refiere la Resolución del Parlamento, que garantice la cobertura de los daños que los robots puedan ocasionar a terceros», toda vez que «la robótica y la IA, por sus particulares características, es una actividad generadora de riesgos a las personas y los bienes y, por tanto, tendrá sentido socializar su cobertura mediante la obligatoriedad de un seguro que garantice la indemnidad de los eventuales perjudicados».

Además, estos perjuicios se han producido de un modo más directo en el momento actual con la situación generada por la pandemia mundial del COVID-19. En este sentido, el Informe Europol: Análisis del Crimen Organizado en Internet - Informe IOCTA 2020¹²⁸ alerta del aumento de la ciberdelincuencia durante la etapa de crisis sanitaria que, en muchos casos, se sirven de estas tecnologías para perpetrar los diferentes delitos. No obstante, como señala el autor citado, este extremo solamente es predicable de aquellos robots que, efectivamente, presenten dicho riesgo de forma considerable, debiendo recibir especial consideración los que transiten por lugares y vías públicas. Precisamente, como hemos tenido ocasión de comprobar, esta ha sido la tendencia acogida por la Resolución de 20 de octubre de 2020 sobre responsabilidad civil y, en su seno, por la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. Así, diferencia entre los sistemas de alto riesgo y aquellos que no presentan dicha característica, existiendo únicamente en el primer caso la obligación de suscribir un seguro.

En otro orden de cosas, debemos reparar acerca de los sujetos que tienen el deber de disponer de estos seguros. Sobre el particular, una solución pasa por pensar que todos los agentes in-

¹²⁷ *Ibid.*, p. 57.

¹²⁸ A este respecto, *vid.* <https://www.dsn.gob.es/es/actualidad/sala-prensa/europol-an%C3%A1lisis-del-crimen-organizado-internet-iocta-2020> (fecha de última consulta 21.02.2021).

tervinientes que puedan, a la postre, ser declarados como responsables deberían suscribir los mismos. Sin embargo, si atendemos a la normativa vigente podemos observar cómo tal conclusión no es acertada. En este sentido, la Directiva sobre responsabilidad por productos defectuosos no indica nada al respecto, por lo que parece que esta exigencia no es predicable para las personas a las que antes aludíamos. Otra cosa será que, voluntariamente, decidan llevarlo a cabo. En esta misma línea, el Real Decreto Legislativo 1/2007 no incorpora este extremo, por lo que el resultado es equivalente al anterior. No obstante, el artículo 131 de la citada norma prevé la posibilidad de que el Gobierno, previa audiencia de los interesados y de las asociaciones de consumidores y usuarios, establezca «un sistema de seguro obligatorio de responsabilidad civil derivada de los daños causados por bienes o servicios defectuosos y un fondo de garantía que cubra, total o parcialmente, los daños consistentes en muerte, intoxicación y lesiones personales».

Al margen de ello, podemos señalar que, como norma general, no existe un deber formal de disponer de un seguro de responsabilidad para el fabricante, productor, distribuidor, proveedor, programador, etc. Sin embargo, como vimos, estas personas podían quedar sujetos a un régimen especial incluido en la Propuesta de Reglamento sobre responsabilidad civil en materia de inteligencia artificial. Así, cuando estos últimos ocupan, al mismo tiempo, la figura de operador, se rigen por las premisas incluidas en la norma referida, con las particularidades que pusimos de relieve.

En cuanto al «fabricante-operador» señalamos que la aplicación de una disposición u otra dependía, fundamentalmente, de que se tratara de un operador inicial o final. En este sentido, si nos encontramos ante un operador inicial que tiene la condición de productor tendremos que recurrir a la Directiva sobre responsabilidad por productos defectuosos y, por ello, no es exigible la suscripción de un seguro.

Por su parte, si se trata de un operador final que es también el productor o si existe un solo operador prevalece la Propuesta de Reglamento y, por tanto, dependerá de la consideración del sistema: si es de alto riesgo, es necesario disponer de un seguro de responsabilidad civil y, por el contrario, si no posee tal carácter, no será obligatorio este extremo.

En otro orden de cosas, cuando se trata de otras personas (distintas al fabricante o productor) y, al mismo, tiempo, son operadores, hemos de estar, de nuevo, a la clasificación del sistema de inteligencia artificial a la que aludíamos. Así, si el mismo es de alto riesgo prevalecerá la Propuesta de Reglamento y, por tanto, será preceptivo contar con un seguro. Si no se trata de esta clase de sistemas, señalamos que, salvo en lo referido a los plazos de prescripción, los importes y el alcance de la indemnización, también debemos acudir a la citada norma. De esta forma, en la línea de lo indicado en la misma, no se requerirá este extremo.

Sobre la exigencia de seguro obligatorio, apunta TAPIA HERMIDA ¹²⁹ que existen distintas dificultades sobre su implantación y «que pueden exponerse en forma de causa y efecto». La causa se identifica con la falta de estadísticas de siniestralidad, ya que «esta ausencia de datos sobre los riesgos asociados a los sistemas de IA, unida a la incertidumbre sobre su evolución en el futuro, dificulta al sector de los seguros elaborar productos de seguro nuevos o adaptados». Por su parte, el efecto «consistirá en el riesgo de que el mercado asegurador diseñe un seguro obligatorio de “talla única” con primas desproporcionadamente elevadas y los incentivos equivocados, alentando a los operadores a optar por el seguro más barato en lugar de por la mejor cobertura, lo que podría convertirse en un obstáculo para la investigación y la innovación».

Por otro lado, tenemos que reflexionar sobre la cobertura del aseguramiento, esto es, el contenido del mismo y, en su caso,

¹²⁹ «La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento», *Revista de Responsabilidad Civil y Seguro*, 2021, p. 93.

las posibles limitaciones aplicables a este sector. Pues bien, tal y como prevé el artículo 73 LCS con la suscripción del seguro de responsabilidad el asegurador se obliga, «dentro de los límites establecidos en la Ley y en el contrato, a cubrir el riesgo del nacimiento a cargo del asegurado de la obligación de indemnizar a un tercero los daños y perjuicios causados por un hecho previsto en el contrato de cuyas consecuencias sea civilmente responsable el asegurado, conforme a derecho». A este respecto, surgen varios aspectos reseñables.

Por un lado, por lo que se refiere al régimen jurídico aplicable a estos seguros hemos de atender al artículo 2 LCS. Este precepto establece, por una parte, el carácter imperativo de los mandatos contenidos en dicha norma y, de otra, una suerte de principio de subsidiariedad (en defecto de ley especial). De esta forma, en primer lugar, tendremos que acudir a las posibles normas específicas existentes y, posteriormente, si existen lagunas, a la Ley 50/1980. De ello se deduce que, si se aprueban normas específicas para regular el aseguramiento la inteligencia artificial (ya sea en general, ya en sector concreto), tendrán preferencia. Asimismo, hemos de traer a colación la distinción¹³⁰ entre los «seguros de régimen común» y los «seguros por grandes riesgos». Para conocer si estamos en un ámbito u otro, debemos centrarnos en la citada Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras y al Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. En concreto, el artículo 11 LOSSEAR determina una serie de «grandes riesgos»¹³¹.

¹³⁰ En este sentido, *vid.* TAPIA HERMIDA, A.J.: «La responsabilidad», *cit.*, pp. 95-96.

¹³¹ Se entienden por seguros de grandes riesgos, entre otros, los referidos a vehículos ferroviarios, aéreos, marítimos, lacustres y fluviales o los de crédito y caución cuando el tomador y el asegurado ejerzan a título profesional una actividad industrial, comercial o liberal y el riesgo se refiera a dicha actividad.

Pues bien, aquellos seguros que reúnan los criterios especificados en el citado precepto se entenderán como seguros por grandes riesgos. Tal y como prevé el artículo 44 LCS, para estos últimos no se ha de acudir al citado artículo 2 LCS y, por tanto, la Ley 50/1980 no es imperativa, sino dispositiva. Por todo lo anterior, el régimen que resulta de aplicación a estos seguros se concreta en la normativa específica que, en su caso, se haya aprobado y en los deberes impuestos por la Ley 20/2015 y por el Real Decreto 1060/2015.

Por su parte, los que no cumplan tales cuestiones serán considerados seguros de régimen común los que, igualmente, se regirán por las disposiciones especiales, si las hubiere. Asimismo, hay que tener en cuenta que, en defecto de tales normas, «los preceptos de la LCS se le aplicarán con carácter imperativo conforme al art. 2 de esa misma LCS. Procede destacar que esta imperatividad busca la protección del tomador y del asegurado, llegando incluso a considerar válidas las cláusulas eventualmente contrarias a dicha Ley pero que sean más beneficiosas para los asegurados¹³²».

Por otro lado, esta protección se manifiesta en «los requisitos que debe cumplir el asegurador, al redactar la póliza, para que las cláusulas eventualmente limitativas de los derechos de los asegurados sean válidamente oponibles a estos. Se trata de los requisitos de resalte en el documento y aceptación específica por el asegurado (art. 3 LCS)¹³³». A este respecto, en cuanto a los límites asegurados debemos tener en cuenta que pueden tener su origen en una ley o bien en el propio clausulado del contrato. No se puede obviar que los contratos de seguro «tienen una serie de límites o delimitaciones que excluyen, en determinadas circunstancias, la obligación de la aseguradora de indemnizar al asegurado¹³⁴».

¹³² Vid. TAPIA HERMIDA, A.J.: «La responsabilidad», *cit.*, p. 95.

¹³³ *Ibidem.*

¹³⁴ ORTIZ FERNÁNDEZ, M.: «Las cláusulas sorprendentes en los contratos de seguro: ¿Delimitación o limitación? A propósito de la STS 732/2017, de 2 de marzo», *Revista Lex Mercatoria*, núm. 7, 2017, pp. 101-102.

Sin embargo, aunque *a priori* puedan parecer cosas equivalentes, «conviene diferenciar entre cláusulas delimitadoras del riesgo y cláusulas limitativas de derechos. Y ello, porque las consecuencias derivadas de encuadrar una cláusula en uno u otro tipo son diferentes». La diferencia fundamental es que las primeras se limitan a concretar el riesgo asegurado, esto es, definen el objeto del contrato y, por su parte, las segundas restringen o modifican los derechos de los asegurados una vez producido el siniestro. Por este motivo, estas últimas están sometidas a un régimen especial cuyo fundamento se encuentra en la necesidad de proteger a los asegurados. Sin entrar en mayores disquisiciones, hemos de tener en cuenta que las citadas cláusulas pueden ser consideradas como «sorpresivas» y que los negocios jurídicos celebrados han de ser sometidos a un «control de transparencia material prohibitivo de las cláusulas sorprendentes»¹³⁵.

Sea como fuere, con ello queremos poner de manifiesto que, para determinar si en un caso el riesgo se encuentra o no cubierto tenemos que atender al tenor literal del negocio jurídico celebrado. En este sentido, no se puede perder de vista la práctica habitual en algunos sectores, ya que puede ser frecuente que, determinados daños no sean satisfechos por las compañías. Pues bien, tal y como pone de relieve TAPIA HERMIDA¹³⁶, no se puede obviar que incluso las compañías más relevantes (tales como Google, Amazon, Microsoft o Tesla) han podido comprobar cómo sus sistemas de inteligencia artificial y de *machine learning* se han mostrado insuficientes y han experimentado distintos errores de seguridad¹³⁷.

¹³⁵ En este sentido, *vid.* MIRANDA SERRANO, L.M.: «Cláusulas limitativas y sorprendentes en contratos de seguro: protección de las expectativas y el consentimiento de los asegurados», *Revista crítica de derecho inmobiliario*, núm. 761, 2017, p. 1172.

¹³⁶ En este sentido, *vid.* <http://ajtapia.com/2020/12/robots-responsables-1-la-responsabilidad-civil-derivada-del-uso-de-la-inteligencia-artificial-y-su-seguro/> (fecha última consulta: 03.01.2021).

¹³⁷ A este respecto, TAPIA HERMIDA alude a los fallos más habituales de los sistemas de inteligencia artificial y aprendizaje automático, que pueden ser de

3. EL CIBERSEGURO COMO POSIBLE MODALIDAD PARA LA INTELIGENCIA ARTIFICIAL Y SUS CARENCIAS: LA NECESIDAD DE CREAR UN SEGURO ESPECÍFICO

De todo lo visto hasta el momento, podemos señalar que el ciberseguro se presenta como la modalidad más adecuada, en principio, para hacer frente a las indemnizaciones que se produzcan en este ámbito. Sobre el particular, indica el autor citado que el seguro cibernético clásico –*existing cyber insurance*– aparece «como la ubicación natural en la que buscar respuestas y soluciones de cobertura; dado que la modalidad principal a través de la cual los sistemas de ML y de AI manipulan los datos es el código y el software¹³⁸». El mismo, se centra en la seguridad de la información, la responsabilidad de la privacidad y la interrupción del negocio.

No obstante, hemos de tener en cuenta que este tipo de seguros recibe distintas denominaciones a pesar de que con ellos se alude a una misma modalidad aseguradora y a unos mismos riesgos. En este sentido, ELGUERO MERINO¹³⁹ señala que, en ocasiones, «es frecuente que la póliza tenga un nombre comercial como producto, además de la denominación —simultánea o alternativa— del seguro en referencia al riesgo asegurado. En este segundo caso, las denominaciones también varían: Seguridad en las

dos tipos: intencionados (*intentional failures*) o casuales (*unintentional failures*). En los primeros, es un agente externo el que produce el error y, por su parte, en los segundos, es el propio sistema el que comete el fallo.

Asimismo, KUMAR, R.S.S./NAGLE, F.: «The Case for AI Insurance», *Harvard Business Review*, 2020. Disponible en <https://hbr.org/2020/04/the-case-for-ai-insurance> (fecha última consulta: 03.01.2021) ponen de manifiesto estas cuestiones y los peligros derivados de los sistemas de inteligencia artificial.

¹³⁸ Vid. <http://ajtapia.com/2020/12/robots-responsables-2-la-responsabilidad-civil-derivada-del-uso-de-la-inteligencia-artificial-y-su-seguro/> (fecha última consulta: 03.01.2021).

¹³⁹ «El seguro de riesgos cibernéticos», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, pp. 379-380.

Redes y Privacidad en los Datos, Seguro de Riesgos Cibernéticos, Security and Privacy, Protección de Riesgos Digitales, Beazley Breach Response, Chubb Cyber Enterprise Risk Management, Hiscox Cyberclear, Seguro de Cyber Riesgos, Riesgos Cibernéticos, Multimedia y de Privacidad de Datos, Cyber Suite Insurance o Cyber Plus Protection, entre otras».

En cuanto al objeto de los mismos, es, en general, tal y como indica el autor referido¹⁴⁰, «proteger la información y los datos que pueden sufrir incidentes en la seguridad de la información», entre los que pueden destacarse la fuga de información, el *ransomware*, el *phising* o la suplantación de identidad. Sea como fuere, no estamos ante un seguro similar a los de responsabilidad civil, ya que no cubre un único riesgo. Muy al contrario, «es una cobertura estructurada según el modelo de póliza de mercado que se utilice». Así, entre las exclusiones generales podemos encontrar los daños personales y materiales o la responsabilidad contractual. Por todo ello, en la práctica, el seguro cibernético al que hacíamos referencia puede no cubrir algunos de los riesgos derivados de la inteligencia artificial.

Sobre el particular, para concluir acerca de si un determinado perjuicio quedaría hipotéticamente dentro de la cobertura del seguro cibernético tradicional, la doctrina¹⁴¹ diferencia entre un total de seis escenarios. A este respecto, señala que únicamente los ataques de robo de modelos –*model stealing attacks*– recibirían am-

¹⁴⁰ *Ibid.*, p. 381. A este respecto, el autor señala que debemos diferenciar entre coberturas generales (gestión de incidentes, responsabilidad por uso y tratamiento de la información, obligaciones en materia de protección de datos, responsabilidad civil frente a terceros, daños propios y defensa y sanciones), extensiones (nuevas filiales, fianzas, periodo informativo y gastos) y coberturas opcionales (gastos de expertos, protección frente a acciones intencionadas de infidelidad por parte de los empleados, defensa ante acciones regulatorias, etc.).

¹⁴¹ *Vid.* <http://ajtapia.com/2020/12/robots-responsables-2-la-responsabilidad-civil-derivada-del-uso-de-la-inteligencia-artificial-y-su-seguro/> (fecha última consulta: 03.01.2021).

paro en el mismo. No ocurre este extremo en los referidos a fuga de datos –*data leakage*– ni en los daños corporales –*bodily harm*–, a la marca –*brand damage*– o a la propiedad física –*damage to physical property*–. Además, las pólizas excluirán la responsabilidad civil derivada de una actuación dolosa del operador o del desarrollo de actividades ajenas al ejercicio de su actividad profesional centrada en la inteligencia artificial, lo que no excluirá la defensa jurídica del mismo frente a reclamaciones¹⁴².

Por todo lo anterior, señala TAPIA HERMIDA que «está emergiendo con fuerza la solución del seguro específico de AI / ML (AI/ML-*specific insurance*)». Así, indica que la necesidad de crear esta modalidad precisa de una actuación urgente por parte de las dos partes interesadas, a saber, las empresas que incorporan estas tecnologías y las compañías aseguradoras. Sea como fuere, lo cierto es que «sigue existiendo una notable incertidumbre acerca de quién lo necesitará y exactamente qué cubrirá» y «es urgente despejar estas incertidumbres porque los eventos recientes han demostrado que los sistemas de AI y ML son frágiles y sus fallos pueden conducir a desastres del mundo real».

De esta suerte, como conclusión hemos de destacar que los seguros actuales se muestran insuficientes para hacer frente a los daños derivados de la inteligencia artificial y el *machine learning*. En este sentido, cobra mayor fuerza la idea de crear una clase *ad hoc* que se configure para dar cobertura a estos peligros. Asimismo, debido a la fragilidad de algunos sistemas, sería muy recomendable que las empresas contaran con un plan de gestión de riesgos¹⁴³ (un *compliance*) que prevea mecanismos para prevenir, controlar y reaccionar frente a los ataques y errores que se produzcan en este ámbito. En todo caso, este sector requiere de una rápida actuación para ofrecer seguridad jurídica a todos los

¹⁴² TAPIA HERMIDA, A.J.: «La responsabilidad», *cit.*, p. 97.

¹⁴³ A este respecto, KUMAR, R.S.S./NAGLE, F.: «The Case», *cit.*, refieren la implantación de este sistema en tres fases (primera semana, primer mes y primer año) con el establecimiento de una serie de actividades a realizar.

sujetos intervinientes y que permita que las compañías aseguradoras puedan responder frente a las potenciales indemnizaciones.

En otro orden de cosas, no se puede obviar que el inciso que señalábamos referido a los límites pactados «da lugar a que el riesgo asegurado deba delimitarse desde varios prismas: geográfica o territorialmente, temporalmente –como las cláusulas *claim made/claim occurrence*–, cuantitativamente –límite agregado, anual, por siniestro, etc.– y causalmente –coberturas globales y específicas, exclusiones legales y convencionales–¹⁴⁴». Desde el punto de vista cuantitativo, es muy importante la suma asegurada que aparece como la cuantía máxima de indemnización. Sin duda, esta suma dependerá del campo concreto de que se trate y variará en función del riesgo existente. Además, para fijar esta última, cobran especial interés las cantidades que recoge la Propuesta de Reglamento, pues operarán como límite máximo de indemnización. Por su parte, en este ámbito cobra especial relevancia la delimitación temporal de los seguros, pues es muy probable que el daño se produzca cuando haya transcurrido un periodo de tiempo razonable desde la actuación del operador.

A este respecto, hemos de tener en cuenta dos acontecimientos, a saber, el hecho causante del daño y el momento de presentación de la reclamación. Como norma general, podemos indicar que quedarán cubiertos los perjuicios que se produzcan como consecuencia de una intervención del operador en la que el seguro se encontraba vigente (con independencia del momento de reclamación). No obstante, la doctrina señala que es posible excepcionar la regla anterior y, por tanto, limitar las indemnizaciones, cuando se cumplan las garantías previstas en el segundo párrafo del artículo 73 LCS. En este sentido, TAPIA HERMIDA¹⁴⁵ diferencia entre dos hipótesis temporales. La primera, en la que no hay duda razonable sobre la cobertura del riesgo, ya que tanto la utilización

¹⁴⁴ ORTIZ FERNÁNDEZ, M.: «Las cláusulas», *cit.*, p. 102.

¹⁴⁵ TAPIA HERMIDA, A.J.: «La responsabilidad», *cit.*, pp. 98-99.

del sistema como la reclamación del perjudicado se producen durante el periodo de vigencia de la póliza. La segunda, en la que no se produce este extremo, porque uno de los dos hechos se ubica fuera del contrato y sí merece una reflexión posterior.

Sobre el particular, el autor citado destaca que «Para permitir la programación en las pólizas de ambas hipótesis y por razones de seguridad jurídica, el legislador introdujo un segundo párrafo en el art. 73 de la LCS para fijar las condiciones de admisibilidad de las cláusulas que delimitan la cobertura de los seguros de responsabilidad civil por referencia a las reclamaciones (las denominadas “claims made”)». De esta suerte, «resulta admisible excluir la cobertura del asegurador mediante la correspondiente cláusula limitativa en la póliza de seguro que deje fuera las reclamaciones realizadas más allá del año siguiente al término del período de seguro o los usos del sistema de inteligencia artificial acaecidos con una antelación superior a un año al inicio de efectos de la póliza».

En la práctica, «las pólizas delimitarán temporalmente el riesgo cubierto por referencia a la presentación formal de la reclamación frente al operador del sistema de inteligencia artificial (mediante comunicación escrita, carta, fax, telegrama, etc.) durante el periodo de vigencia de la póliza, con independencia de que el hecho causante se haya producido antes de la vigencia de la póliza (siempre que fuera desconocido) o durante dicha vigencia». Sea como fuere, esta posibilidad solamente es aplicable cuando se haya pactado expresamente, pues, en otro caso, recurriremos a la norma antes reseñada.

Para finalizar con esta referencia al aseguramiento, resta realizar dos apuntes. De un lado, que la doctrina científica¹⁴⁶ apunta que, debido a la importancia cuantitativa y cualitativa de esta cobertura, quizás lo más recomendable es, en ciertos supuestos, recurrir a la figura del coaseguro (art. 33 LCS). De otro lado, en el campo de la digitalización financiera, adquiere especial relevancia

¹⁴⁶ TAPIA HERMIDA, A.J.: «La responsabilidad», *cit.*, p. 94.

el principio de cobertura preventiva. A este respecto, cabe reseñar la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero al regular los espacios controlados de pruebas. Esta disposición se ocupa de regular «un entorno controlado de pruebas que permita llevar a la práctica proyectos tecnológicos de innovación en el sistema financiero con pleno acomodo en el marco legal y supervisor, respetando en todo caso el principio de no discriminación» (art. 1 ley 7/2020). Además, la norma «refuerza los instrumentos necesarios para garantizar los objetivos de la política financiera en el contexto de la transformación digital» y, a tal efecto, dota de instrumentos a las autoridades competentes, a los promotores de innovaciones de base tecnológica aplicables en el sistema financiero y a los usuarios para comprender adecuadamente las implicaciones de la transformación digital (art. 1 párrafo segundo Ley 7/2020).

4. LA RELEVANCIA DE DISPONER DE UN REGISTRO Y DE ESTABLECER FONDOS DE COMPENSACIÓN

Por último, hemos de destacar el papel que, a este respecto, pueden desempeñar los fondos de compensación y la importancia de que existan registros para favorecer la publicidad (tanto de las personas y empresas que han contribuido en la realización de la máquina como de los seguros suscritos). Como vimos, se hace referencia a estos extremos en distintos instrumentos europeos. La Resolución del Parlamento Europeo, de 16 de febrero de 2017, ya preveía la necesidad de que se crease un «sistema global de registro de robots avanzados» dentro del mercado interior de la Unión cuando fuese necesario. En este sentido, destaca la doctrina¹⁴⁷ que, «si finalmente se crea un sistema de aseguramiento

¹⁴⁷ En este sentido, *vid.* BADILLO ARIAS, J.A.: «Responsabilidad civil», *cit.*, p. 37. Asimismo, DÍAZ ALABART, S.: *Robots y responsabilidad civil*, Madrid, Reus,

obligatorio de robots inteligentes, es necesario la creación de un registro también obligatorio de robots, con el fin, en este caso, de saber cuáles serían objeto de dicho aseguramiento, así como quién es su fabricante, propietario o usuario, sus características técnicas, inspecciones o revisiones, etc.».

Asimismo, se recogía la necesidad de que, en aquellos casos en los que no concurriese un seguro obligatorio, existiera un fondo de compensación que, en última instancia, asegurase el resarcimiento de las víctimas. En suma, este fondo, al igual que en otros ámbitos, compensaría a las víctimas de aquellos daños que, o bien no pudieran ser determinados, o bien no pudiera asumir el responsable. Igualmente, se incluía la necesidad de crear un número de matrícula individual que asegurase la asociación entre el robot y el fondo del que dependiera y que permitiese que cualquier persona que interactuase con el mismo tuviera constancia de la naturaleza del fondo, los límites de su responsabilidad en caso de daños materiales, los nombres y las funciones de los participantes y otros datos pertinentes.

Sobre el particular, algunos autores¹⁴⁸ señalan que de esta Resolución cabe extraer que el legislador se está refiriendo a dos tipos de fondo de compensación: de un lado, el que cubriría los perjuicios causados por robots que no disponen de seguro de responsabilidad civil y, de otro lado, el que compensa los daños ocasionados, de tal forma que, de algún modo, limita la responsabilidad de los sujetos intervinientes y de las compañías aseguradoras. En todo caso, como muy acertadamente destacan a nuestro parecer, ambos podrían complementarse y dar lugar a un único fondo de compensación.

En esta línea, el precitado informe del grupo de expertos «Liability for Artificial Intelligence and other emerging techno-

2018, p. 81 pone de relieve que este registro de robots puede emplearse para otros fines.

¹⁴⁸ Vid. BADILLO ARIAS, J.A.: «Responsabilidad civil», *cit.*, p. 59.

logies» destaca que los mismos pueden usarse para proteger a los perjudicados que tienen derecho a una compensación de acuerdo con las reglas de responsabilidad aplicables, pero cuyas reclamaciones no pueden satisfacerse. Por su parte, la Resolución de 20 de octubre de 2020 sobre responsabilidad civil, consciente de la dificultad a la que se han de enfrentar las compañías de seguros para financiar las elevadas indemnizaciones indica que es difícil concebir una solución de «talla única» y que «el mercado de los seguros necesitará tiempo para adaptarse». Por ello, indica en su Considerando 22 que «En casos excepcionales, como en el caso de que se produzcan daños colectivos, en los que la indemnización exceda de modo significativo los importes máximos establecidos en el presente Reglamento, debe alentarse a los Estados miembros a crear un fondo especial de indemnización para un período de tiempo limitado que responda a las necesidades específicas de esos casos».

Asimismo, destaca que «También podrían crearse fondos especiales de indemnización para cubrir aquellos casos excepcionales en los que un sistema de IA, que aún no esté clasificado como sistema de IA de alto riesgo y que, por tanto, todavía no está asegurado, cause daños o perjuicios».

Desde nuestra perspectiva, entendemos que estos registros pueden resultar fundamentales para que las personas que sufren daños derivados del uso de esta tecnología obtengan una reparación adecuada. Además, contribuye a impulsar la confianza depositada por los sujetos a la hora de aproximarse a estas máquinas, ya que podrían conocer, en definitiva, una serie de información que, a la postre, puede ser imprescindible. Por otro lado, desde nuestra perspectiva, resulta muy favorable que se establezcan seguros y fondos de compensación para asegurar el resarcimiento de las víctimas¹⁴⁹. Es cierto que imponer la suscripción de los primeros

¹⁴⁹ En esta línea, *vid.* OROZCO GONZÁLEZ, M.: «Reflexiones acerca de la relación entre Inteligencia Artificial y robótica», en *Cuestiones clásicas y actuales*

de manera forzosa puede ser excesivamente gravoso y desincentivar el avance de la tecnología¹⁵⁰, pero en ciertas aplicaciones de la inteligencia artificial ha de ser un requisito indispensable (al igual que ocurre en otros sectores). Por su parte, en cuanto al fondo de compensación, quedan por resolver algunas cuestiones tales como la forma en la que se ha de financiar, si existirá uno a nivel europeo y/o se crearán varios *ad hoc* en cada uno de los estados o si será, en todos los casos, obligatorio.

En definitiva, podemos llevar a cabo una asimilación a dos figuras existentes en el ámbito de los automóviles: el Fichero de Vehículos Asegurados (FIVA) y el Consorcio de Compensación de Seguros. Así, se trataría de extrapolar, *mutatis mutandi*, estas realidades al ámbito de la inteligencia artificial con el objetivo último de favorecer la transparencia, el conocimiento y, en última instancia, establecer un resarcimiento adecuado para las víctimas de los perjuicios¹⁵¹.

del Derecho de Daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón (Coord. J. ATAZ LÓPEZ/J.A. COBACHO GÓMEZ), Navarra, Aranzadi, 2021, p. 875.

¹⁵⁰ En este sentido, *vid.* BERTOLINI, A.: «Insurance and Risk Management for Robotic Devices: Identifying the Problems», *Global Jurist*, vol.3, núm. 16, 2016, pp. 291-314; BERTOLINI, A., *et al.*: «On Robots and Insurance», *International Journal of Social Robotics*, núm. 8, 2016, pp. 381-391.

¹⁵¹ Para más información, *vid.* BADILLO ARIAS, J.A.: «Responsabilidad civil», *cit.*, pp. 59-62.

VI.

REFERENCIAS BIBLIOGRÁFICAS

- ABRAHAM, K.S./RABIN, R.L.: «Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era», *Virginia Law Review*, vol. 105, 2019, pp. 127-171.
- ATIENZA NAVARRO, M.L.: «Una aproximación a la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial de 27 de abril de 2020», *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 54, 2020.
- BADILLO ARIAS, J.A.: «Responsabilidad civil y aseguramiento obligatorio de los robots», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, pp. 25-66.
- BARRIO ANDRÉS, M.: «Del Derecho de Internet al Derecho de los Robots», en *Derecho de los Robots* (Dir. M. BARRIO ANDRÉS), Madrid, Wolters Kluwer, 2018, pp. 61-86.
- *Manual de Derecho Digital*, Valencia, Tirant lo Blanch, 2020.
- BERTOLINI, A.: «Insurance and Risk Management for Robotic Devices: Identifying the Problems», *Global Jurist*, vol.3, núm. 16, 2016, pp. 291-314.
- BERTOLINI, A., *et al.*: «On Robots and Insurance», *International Journal of Social Robotics*, núm. 8, 2016, pp. 381-391.

- BLAIKIE, D./DONOVAN, N.: «New ICO guidance on AI: privacy by design saves retrofitting later», *Practical Law UK Articles*, 2020, pp. 1-4.
- BLAS ORBÁN, C.: «Contagio transfusional de VHC. Reflexiones sobre la previsibilidad del daño», *DS*, vol. 16, núm. 2, 2008, pp. 179-216.
- BODEN, M.A.: *Inteligencia artificial*, Madrid, Turner, 2017.
- CALZADA CONDE, M.A.: *El seguro de responsabilidad civil*, Navarra, Aranzadi, 2005.
- CASTELLS I MARQUÈS, M.: «Drones recreativos: normativa aplicable, responsabilidad civil y protección de datos», *Revista de Derecho Civil*, vol. VI, núm. 1, 2019, pp. 297-333.
- ČERKA, P./GRIGIENĖ, J./SIRBIKYTĖ, G.: «Liability for damages caused by artificial intelligence», *Computer Law & Security Review*, vol. 31, núm. 3, 2015, pp. 376-389.
- CHURNIN, S.: *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*, Madrid, Servicio de Publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, 2011.
- CLARK, B./WILKINSON-DUFFY, R.: «AI and trade mark law: keeping up with the robots», *Practical Law UK Articles*, 2020, pp. 1-12.
- COHEN, I.G.: «Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?», *Georgetown Law Journal*, vol. 108, 2020, pp. 1425-1469.
- CONWAY, J./FRITH, G.: «The rise of the deepfake: looking into a dystopian future?», *Practical Law UK Articles*, 2020, pp. 1-14.
- CULLELL MARCH, C.: «El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico», *IDP. Revista de Internet, Derecho y Política*, núm. 11, 2010, pp. 1-10.
- DE LAS HERAS GARCÍA, M.A.: «*Lex Artis, Onus Probandi* y responsabilidad médica», *Revista jurídica de la Región de Murcia*, núm. 36, 2005, pp. 13-68.
- DÍAZ ALABART, S.: *Robots y responsabilidad civil*, Madrid, Reus, 2018.
- ELGUERO MERINO, J.M.: «El seguro de riesgos cibernéticos», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, pp. 375-409.

- ERCILLA GARCÍA, J.: *Normas de Derecho Civil y Robótica. Robots Inteligentes, Personalidad Jurídica, Responsabilidad Civil y Regulación*, Navarra, Aranzadi, 2018.
- EVANS, B.J./PASQUALE, F.: «Product Liability Suits dor FDA-Regulated AI/ML Software», *SSRN*, 2020, pp. 1-15.
- FERREIRA, A.E.: «Partilhar o mundo com robôs autônomos: a responsabilidade civil extracontratual por danos. introdução ao problema», *Cuestiones de Interés Jurídico*, IDIBE, 2017, pp. 1-32.
- FOUNTOUKAKOS, K., *et al.*: «European Commission strategy for data and AI: shaping a digital future», *Practical Law UK Articles*, 2020, pp. 1-5.
- GARCÍA-PRIETO CUESTA, J.: «¿Qué es un robot?», en *Derecho de los robots* (Dir. M. BARRIO ANDRÉS), Madrid, Wolters Kluwer, 2018, pp. 25-60.
- GARCÍA TERUEL, R.M.: «El derecho de daños ante la inteligencia artificial y el *machine learning*: una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea», en *Cuestiones clásicas y actuales del Derecho de Daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón* (Coord. J. ATAZ LÓPEZ/J.A. COBACHO GÓMEZ), Navarra, Aranzadi, 2021, pp. 1009-1055.
- GÓMEZ ABEJA, L.: «Consentimiento informado y derechos fundamentales», *Revista Europea de Derechos Fundamentales*, núm. 18, 2011, pp. 275-306.
- GÓMEZ LIGÜERRE, C./GABRIEL GARCÍA-MICÓ, T.: «Liability for Artificial Intelligence and other emerging technologies», *InDret*, núm. 1, 2020, pp. 501-511.
- GONZÁLEZ VALVERDE, A.: «Responsabilidad por el potencial sesgo discriminatorio de los algoritmos de los productos de Inteligencia Artificial. A propósito de la *Algorithmic Accountability Act of 2019 (s.1108)*», en *Cuestiones clásicas y actuales del Derecho de Daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón* (Coord. J. ATAZ LÓPEZ/J.A. COBACHO GÓMEZ), Navarra, Aranzadi, 2021, pp. 1125-1273.

- HACKER, P./KRESTEL, R./GRUNDMANN, S./NAUMANN, F.: «Explainable AI under contract and tort law: legal incentives and technical challenges», *Artificial Intelligence and Law*, vol. 28, 2020, pp. 415-439.
- HOLME, D.: «Using artificial intelligence: not pie in the sky», *Practical Law UK Articles*, 2017, pp. 1-3.
- IBÁÑEZ-GUZMÁN J./LAUGIER C./YODER J.D./THRUN S.: «Autonomous Driving: Context and State-of-the-Art», en *Handbook of Intelligent Vehicles* (edit. A. ESKANDARIAN), Londres, Springer, 2012, pp. 1271-1310.
- JAUME-PALASÍ, L.: «Cómo la inteligencia artificial está impactando en las sociedades», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 27-39.
- KANE, G.C./PHILLIPS, A.N./COPULSKY, J.R.: *The Technology Fallacy: How People Are the Real Key to Digital Transformation*, Massachusetts, MIT Press, 2019.
- KEMP, R.: «Artificial Intelligence: introduction», *Practical Law UK Articles*, 2017.
- «Legal Aspects of Artificial Intelligence», 2018, p. 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 última consulta: 03.01.2021).
- KEMP, R./MOYNIHAN, D./KEMP, C.: «IP in AI-generated works, datasets and trade secrets», *Practical Law UK Articles*, 2020, pp. 1-9.
- KUMAR, R.S.S./NAGLE, F.: «The Case for AI Insurance», *Harvard Business Review*, 2020. Disponible en <https://hbr.org/2020/04/the-case-for-ai-insurance> (fecha última consulta: 03.01.2021).
- KURZWEIL, R.: *The singularity is near. When humans transcend biology*, New York, Penguin Group, 2005.
- LACRUZ MANTECÓN, M.L.: «Inteligencia artificial y coches autónomos: análisis jurídicos europeos», *Revista Crítica de Derecho Inmobiliario*, núm. 775, 2019, pp. 2373-2409.
- «Cibernética y Derecho europeo: ¿una inteligencia robótica?», *Diario La Ley*, núm. 9376, 2019, pp. 1-19.

- *Robots y personas. Una aproximación jurídica a la subjetividad cibernética*, Madrid, Reus, 2020.
- LIN, P./ABNEY, K./BEKEY, G.A.: *Robot Ethics: The Ethical and Social Implications of Robotics*, Massachusetts, The MIT Press, 2012.
- LÓPEZ-COBO, C.: *El seguro de responsabilidad civil. Fundamentos y modalidades*, Madrid, Libros Tobal, 1988.
- MCCARTHY, J., *et al.*: «A proposal for the dartmouth summer research project on artificial intelligence», 1955, pp. 1-13. Disponible en: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> (fecha última consulta: 03.01.2021).
- MIRANDA SERRANO, L.M.: «Cláusulas limitativas y sorprendentes en contratos de seguro: protección de las expectativas y el consentimiento de los asegurados», *Revista crítica de derecho inmobiliario*, núm. 761, 2017, pp. 1151-1196.
- MONTERROSO CASADO, E.: «Repercusiones de la inteligencia artificial en el ámbito de la responsabilidad civil», *Revista de responsabilidad civil, circulación y seguro*, núm. 11, 2010, pp. 6-20.
- MUGA MUÑOZ, J.L.: «La responsabilidad patrimonial de las administraciones públicas por el contagio de sida», *RAP*, núm. 136, 1995, pp. 277-308.
- MUÑOZ VILLAREAL, A./GALLEGO CORCHERO, V.: «Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad a los robots», en *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (Dir. E. MONTERROSO CASADO/Coord. A. MUÑOZ VILLAREAL), Valencia, Tirant lo Blanch, 2019, pp. 67-100.
- MURPHY, R.R.: *Introduction to AI Robotics*, Massachusetts, The MIT Press, 2019.
- NAPPERT, S.: «The challenge of artificial intelligence in arbitral decision-making», *Practical Law UK Articles*, 2018, pp. 1-7.
- NÚÑEZ ZORRILLA, M.C.: «Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial», *Revista española de derecho europeo*, núm. 66, 2018, pp. 9-53.

- *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, Madrid, Reus, 2019.
- OROZCO GONZÁLEZ, M.: «Reflexiones acerca de la relación entre Inteligencia Artificial y robótica», en *Cuestiones clásicas y actuales del Derecho de Daños. Estudios en Homenaje al Profesor Dr. Roca Guillaumón* (Coord. J. ATAZ LÓPEZ/J.A. COBACHO GÓMEZ), Navarra, Aranzadi, 2021, pp. 861-876.
- ORTIZ FERNÁNDEZ, M.: «Las cláusulas sorpresivas en los contratos de seguro: ¿Delimitación o limitación? A propósito de la STS 732/2017, de 2 de marzo», *Revista Lex Mercatoria*, núm. 7, 2017, pp. 101-118.
- MARTÍN OSANTE, J.M.: *El seguro de responsabilidad civil empresarial*, Madrid, Marcial Pons, 2018.
- NAVAS NAVARRO, S.: «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)*, Granada, Comares, 2021, pp. 1-50.
- NÚÑEZ ZORRILLA, M.C.: *Inteligencia artificial y responsabilidad civil*, Madrid, Reus, 2019.
- PARRA LUCÁN, M.A.: *Daños por productos y protección del consumidor*, Bosch, Barcelona, 1990.
- «La compatibilidad de la directiva de responsabilidad por productos defectuosos y los regímenes de responsabilidad especiales “existentes” en el momento de su notificación», *Revista CESCO de Derecho de Consumo*, núm. 13, 2015, pp. 134-143.
- PAVELEK ZAMORA, E.: «Seguros obligatorios y obligación de asegurarse», *Revista española de seguros: Publicación doctrinal de Derecho y Economía de los Seguros privados*, núm. 106, 2001, pp. 235-276.
- PAVELEK ZAMORA, E./CAÑIZARES RUBINI, F.: «La responsabilidad civil patronal y su aseguramiento», en *Estudios sobre el aseguramiento de la responsabilidad en la gran empresa* (Dir. F.J. SÁNCHEZ CALERO), Madrid, Musini, SA, 1994, pp. 239-318.
- PEGUERA POCH, M.: «En búsqueda de un marco normativo para la Inteligencia Artificial», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 41-56.

- PERÁN ORTEGA, J.: *La responsabilidad civil y su seguro*, Madrid, Tecnos, 1998.
- RAMÓN FERNÁNDEZ, F.: «Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?», *Diario La Ley*, núm. 9365, 2019.
- REGLERO CAMPOS, L.F.: «El seguro de responsabilidad civil», en *Tratado de responsabilidad civil* (Coord. L.F. REGLERO CAMPOS/J.M. BUSTO LAGO), 5ª edic., t. I, Navarra, Aranzadi, 2014, pp. 1363-1554.
- RUBÍ PUIG, A.: «Retos de la inteligencia artificial y adaptabilidad del derecho de daños», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 57-71.
- SEBASTIÁN CÁRDENAS, M.L.: «Fallo humano: la quiebra de un paradigma», *Apuntes de Psicología*, vol. 27, núm. 1, 2009, pp. 21-51.
- SELBST, A.D.: «Negligence and AI's Human Users», *Boston University Law Review*, vol. 100, 2020, pp. 1315-1376.
- SOLAR CAYÓN, J.I.: *La Inteligencia Artificial Jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Navarra, Aranzadi, 2019.
- SOUSA ANTUNES, H.: «Civil liability applicable to artificial intelligence: a preliminary critique of the European Parliament Resolution of 2020», *SSRN*, 2020, pp. 1-23.
- STEPHENS, K./BOND, T.: «Artificial intelligence: navigating the IP challenges», *Practical Law UK Articles*, 2018, pp. 1-14.
- SUMROY, R./DONOVAN, N.: «AI and data protection: balancing tensions», *Practical Law UK Articles*, 2019, pp. 1-16.
- TAPIA HERMIDA, A.J.: «Seguro de responsabilidad civil», en *Estudios sobre el contrato de seguro* (Dir. M.R. QUINTÁNS-EIRAS/L. RAMÍREZ OTERO), Perú, Universidad de Piura, 2017, pp. 599-623.
- «Decálogo de la inteligencia artificial ética y responsable en la Unión Europea», *Diario La Ley*, núm. 9749, sección Tribuna, 2020, pp. 1-7.
- «La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento», *Revista de Responsabilidad Civil y Seguro*, 2021, pp. 79-104.

- TORRUBIA CHALMETA, B.: «Aeronaves civiles no tripuladas. Contexto y regulación», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 255-267.
- TURING, A.: «Computing Machinery and Intelligence», *Mind*, vol. LIX, núm. 236, 1950, pp. 433-460.
- VILASAU I SOLANA, M.: «La realización de perfiles y la salvaguardia de los derechos y libertades del afectado», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 181-202.
- WAGNER, G.: «Robot Liability», en *Liability for Artificial Intelligence and the Internet of Things* (edit. S. LOHSSE/R. SCHULZE/D. STAUDENMEYER), Baden-Baden, Nomos, 2019, pp. 27-62.
- WICKENS, C.D.: *Engineering psychology and human performans*. Nueva York, Harper Collins, 1992.
- XALABARDER, R.: «Inteligencia artificial y propiedad intelectual», en *Retos jurídicos de la inteligencia artificial*, Navarra, Aranzadi, 2020, pp. 205-223.
- ZAPATA SEVILLA, J.: «Inteligencia artificial y responsabilidad civil: el caso de las organizaciones descentralizadas autónomas», 2019, pp. 1-15. Disponible en: <https://riuma.uma.es/xmlui/bitstream/handle/10630/18645/Inteligencia%20artificial%20y%20responsabilidad%20civil%20Oviedo%20%28Comunicaci%C3%B3n%20Jos%C3%A9%20Zapata%20Sevilla%29.pdf?sequence=1> (fecha última consulta: 03.01.2021).
- ZURITA MARTÍN, I.M.: *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Madrid, Reus, 2020.

GRACIAS POR CONFIAR EN NUESTRAS PUBLICACIONES

Al comprar este libro le damos la posibilidad de consultar gratuitamente la versión ebook.

Cómo acceder al ebook:

- ☞ **Acceda a nuestra página web**, sección Acceso ebook
(www.dykinson.com/acceso_ebook)
- ☞ **Rellene el formulario** que encontrará facilitando, el código de acceso que le facilitamos a continuación así como los datos con los que quiere acceder al libro en el futuro (correo electrónico y contraseña de acceso).
- ☞ Si ya es **cliente registrado**, deberá acceder con su **correo electrónico y contraseña habitual**.
- ☞ Una vez registrado, **acceda a la sección Mis e-books de su cuenta de cliente**, donde encontrará la versión electrónica de esta obra ya desbloqueada para su uso.
- ☞ Para acceder al libro en el futuro, ya sólo es necesario que se identifique en nuestra web con su correo electrónico y su contraseña, y que se dirija a la sección Mis ebooks de su cuenta de cliente.



CÓDIGO DE ACCESO

Rasque para ver el código

Nota importante: Sólo está permitido el uso individual y privado de este código de acceso. Está prohibida la puesta a disposición de esta obra a una comunidad de usuarios.

**MANTÉNGASE INFORMADO
DE LAS NUEVAS PUBLICACIONES**

**Suscríbese gratis
al boletín informativo
www.dykinson.com**

Y benefíciense de nuestras ofertas semanales