Capítulo III

REGLAS ESPECIALES DE RESPONSABILIDAD CIVIL EN CASO DE DAÑOS OCASIONADOS POR SISTEMAS DE INTELIGENCIA ARTIFICIAL. FUTURA NORMATIVA EUROPEA Y DERECHO VIGENTE

El ingente trabajo de las diferentes instancias europeas acerca de una posible regulación de la IA y que ha culminado, por ahora, en la AIA, así como la inmensa e inabarcable producción de documentos hace difícil a cualquiera no perderse entre ellos a la hora de abordar esta materia [80]. Por eso, en el presente capítulo voy a presentar la Propuesta del Parlamento europeo sobre un régimen especial de responsabilidad civil en materia de IA de 20 de octubre de 2020 combinando su presentación (II.), por un lado, con las recomendaciones dadas en su informe por el *Expert Group on Liability and New Technologies* (NTF), y, por otro, con las soluciones que se pueden adoptar a partir del derecho español vigente mientras esta Propuesta no se convierta en Reglamento (III.). Primero, no obstante, quiero dejar constancia de los principales instrumentos jurídicos elaborados por las diferentes instancias europeas (I.).

I. Principales instrumentos jurídicos

Como se sabe, el 16 de febrero de 2017, el Parlamento de la UE adoptó una *Resolución sobre normas de derecho civil sobre robótica con recomendaciones a la Comisión*. En esta Resolución pidió a la Comisión que presentara una

[80] Como acertadamente destaca Isabel Zurita Martín, «Las propuestas de reforma legislativa del Libro Blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil», *Actualidad Jurídica Iberoamericana*, núm. 14, febrero 2021, pp. 438-487.

propuesta de instrumento legislativo con la finalidad de establecer unas normas de derecho civil sobre la responsabilidad de los robots y de la IA.

El año 2018 fue muy activo en este ámbito. De hecho, en febrero, el Servicio de Investigación del Parlamento Europeo (EPRS) publicó un estudio acerca de *Un enfoque común de la UE sobre las normas de responsabilidad y el seguro para vehículos conectados y autónomos*[81]. El 25 de abril de 2018, la Comisión publicó un documento de trabajo de los servicios sobre *Responsabilidad por las tecnologías digitales emergentes*[82] que acompaña al documento *Inteligencia artificial para Europa*[83].

En marzo de 2018, la Comisión Europea creó el tantas veces, a lo largo de este trabajo, citado, Grupo de Expertos de alto nivel en Responsabilidad y Nuevas Tecnologías con dos formaciones: NTF («New Technologies Formation») y PLDF («Products Liability Directive Formation»). El NTF debe limitarse a cuestiones de responsabilidad extracontractual. Después de analizar las leyes nacionales relevantes, observar casos específicos y comparar diferentes aspectos de los regímenes de responsabilidad nacionales y de la UE actuales, un Informe presenta los hallazgos de la NTF. El Informe sobre *Responsabilidad por la Inteligencia Artificial y otras tecnologías digitales emergentes* ha supuesto un hito significativo, cuya finalidad es establecer recomendaciones para regular un régimen especial de responsabilidad civil en caso de daños ocasionados por la IA.

A este Informe le siguen otros documentos importantes, que ayudan a comprender cuál es el marco legal que la UE tiene en mente cuando se trata de la responsabilidad civil de la IA. En particular, citaré tres de ellos: el *Informe sobre las implicaciones de seguridad y responsabilidad de la Inteligencia Artificial, Internet de las Cosas y la robótica*[84], el Libro blanco *Sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza*[85] y la Resolución del Par-

[81] <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf>. Fecha de la consulta: mayo 2022.

[82] SWD(2018) 137 final.

[83] COM(2018) 237 final.

[84] COM(2020) 64 final, 19.2.2020.

[85] COM(2020) 65 final, 19.2.2020.

lamento europeo de 20 de octubre de 2020 con una *Propuesta de Reglamento en materia de responsabilidad civil por el uso de inteligencia artificial*[86]. Más reciente en el tiempo, si bien no trata la materia de la responsabilidad civil, sino los requisitos necesarios para que un sistema de IA puede ponerse en circulación en el mercado de forma segura, es la ya citada AIA, de la que ya se conocen dos textos de compromiso que iré citando en este trabajo en los lugares oportunos. Sí que hace, en cambio, una clasificación de los sistemas de IA en función del riesgo sobre la que volveré posteriormente.

Por último, desde la Resolución del Parlamento de 2017 anteriormente citada, la UE ha venido destacando que la Ética no debería estar ausente de este debate. En mi opinión, los documentos más relevantes son, en primer lugar, el elaborado por el Grupo de expertos de alto nivel en IA, *Directrices éticas para una IA fiable*[87], documento hecho público el 8 de abril de 2019 y, en segundo lugar, la Comunicación de la Comisión sobre *Fomento de la confianza en la inteligencia artificial centrada en el ser humano*[88]. De todos modos, existen numerosos documentos de diversas organizaciones donde se elaboran —y se adoptan por sus miembros— principios éticos en materia de IA[89]. Uno de los que más han influido en la regulación proyectada de la IA es el Informe de la *Datenethikkommission*[90] acerca del uso de los datos y de la IA en nuestra economía y sociedad. Otra cuestión es el papel que los principios éticos desempeñan en el debate sobre la IA. En mi opinión, cubren un espacio hasta que los legisladores decidan publicar normas reguladoras

[86] <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html>. Fecha de la consulta: mayo 2022.

[87] <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Fecha de la consulta: mayo 2022.

[88] COM(2019) 168 final.

[89] Fjeld *et al., Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, Berkman Klein Center for internet & society at Harvard University, Research publication núm. 2020-1, 15 enero 2020. Online: <https://cyber.harvard.edu/publication/2020/principled-ai>. Fecha de la consulta: mayo 2022.

[90] <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=DC492965701F1183E8BF3C1C32300AAF.1_cid364?__blob=publicationFile&v=6>. Fecha de la consulta: mayo 2022.

de aquélla. Es decir, proporcionan un marco de seguridad y fiabilidad para todos los sujetos involucrados, es decir, para los fabricantes de sistemas de IA, operadores, usuarios y consumidores finales mientras no exista norma jurídica aplicable, la cual podrá, en su caso, replicarlos, matizarlos, concretizarlos o establecer lo contrario [91]. Estos principios podrán plasmarse asimismo en códigos de conducta.

En cualquier caso, no voy a tratar cuestiones relacionadas con los principios éticos para una IA confiable. Me centraré tan solo en los aspectos jurídicos de relieve en materia de responsabilidad civil.

II. Aspectos jurídicos relevantes en materia de responsabilidad civil

En relación con los diferentes aspectos jurídicos de interés en relación con la responsabilidad civil por una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA (art. 2.1 Propuesta de reglamento 2020) voy a destacar, por un lado, la diferencia entre sistemas de «alto» y «bajo» riesgo (1.), su mal funcionamiento (2.) y, por otro, los dos regímenes de responsabilidad civil previstos en caso de daños por su funcionamiento el cual es operado por un nuevo sujeto responsable, cual es el denominado «operador» (3.), a los que añadiré algunos aspectos relacionados con la prueba (4.).

1. Sistemas de «alto» y «bajo» riesgo. La Propuesta de reglamento de un régimen de responsabilidad civil en materia de inteligencia artificial y su relación con la Artificial Intelligence Act

Los textos europeos citados en relación con la responsabilidad civil por el uso de sistemas de IA distinguen entre tecnología de «alto riesgo» [92] (por ejemplo, automóviles sin conductor, drones, un brazo quirúrgico robotizado [93])

[91] Florian Möslein, «Die normative Kraft des Ethischen – Ein Fallbeispiel zur Effektivität von Leitlinien für Künstliche Intelligenz», *Recht Digital*, 1/2020, pp. 34-40.

[92] *Libro Blanco en IA*, pp. 16-17.

[93] Susana Navas Navarro (dir.), *Salud e Inteligencia artificial desde el Derecho privado*, Comares, Granada, 2021.

y la tecnología de «bajo riesgo» (por ejemplo, una aspiradora como Roomba, un chatbot como Alexa, algunas de las herramientas LegalTech).

La Propuesta de reglamento 2020, en consonancia con el *Libro Blanco en IA,* solo define el sistema de IA de alto riesgo de suerte que el de bajo riesgo se define en negativo, es decir, es aquel sistema que no es de alto riesgo. Pues bien, en la Propuesta se advierte que un sistema de IA debe considerarse de alto riesgo cuando: «el potencial significativo en un sistema de IA que funciona de forma autónoma para causar daños o perjuicios a una o más personas de manera aleatoria y que excede lo que cabe esperar razonablemente; la magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza el sistema de IA» (art. 3 letra c Propuesta de reglamento 2020)[94]. Es lo que se conoce como *significant harm*, expresión empleada en el Derecho norteamericano de la responsabilidad civil del fabricante por productos defectuosos[95], pero que no deja de plantear cuestiones por su excesiva ambigüedad[96]. Además, la Propuesta de reglamento 2020 ofrece una definición de «daño o perjuicio», en su art. 3 letra i, en la que establece como tal: «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».

La descripción del sistema de IA de alto riesgo parece pensar en daños que se producen en espacios públicos donde existe la posibilidad de que se produzcan potencialmente no solo daños individuales que afectan a una o varias personas (por ejemplo, las víctimas de un accidente con un coche autónomo) sino también que se produzcan «daños colectivos» que pueden afectar a la sociedad o a la economía en general (v. gr. manipulación del com-

[94] Gerhard Wagner, «Haftung für Künstliche Intelligenz – Eine Gesetzinitiative des Europäischen Parlaments», *ZEuP*, 2021, p. 554.

[95] Mark A. Geistfeld, *Principles of Products Liability*, Nueva York, Foundation Press, 2011, pp. 115 ss.

[96] Andrea Bertolini, «Artificial Intelligence and Civil Liability», Study requested by the JURI Committee, European Parliament, July, 2020, p. 77.

portamiento de los votantes, suministro de información mediante un asistente virtual acerca de una información que es errónea y conduce a daños físicos a un gran número de personas).

En un anexo al Reglamento se pretenden enumerar los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan (art. 4.2 de la Propuesta de reglamento 2020). De hecho, el *Libro Blanco en IA* hacía referencia a los sectores que consideraba críticos como el transporte o la asistencia[97], dentro de la cual, se podría comprender el sector de la sanidad. El reciente *Draft Report*

[97] *Libro Blanco en IA*, pp. 16-17: Un sistema de IA puede considerarse de alto riesgo o de riesgo elevado cuando se cumplan los criterios siguientes:

- En primer lugar, que la aplicación de IA se emplee en un sector en el que, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos. El primer criterio vela por que la intervención reguladora se centre en aquellas áreas en las que, de manera general, se considere que hay más probabilidad de que surjan riesgos. En el nuevo marco regulador deben detallarse de manera específica y exhaustiva los sectores que englobe. Por ejemplo, la sanidad, el transporte, la energía y determinados ámbitos del sector público. Esta lista debe revisarse periódicamente y modificarse cuando proceda en función de los desarrollos pertinentes en la práctica.
- En segundo lugar, que la aplicación de IA en el sector en cuestión se use, además, de manera que puedan surgir riesgos significativos. Este segundo criterio refleja el reconocimiento de que no toda utilización de la IA en los sectores señalados implica necesariamente riesgos significativos. Por ejemplo, si bien la atención sanitaria puede ser un sector importante, un fallo en el sistema de asignación de citas de un hospital no supondrá en principio un riesgo significativo que justifique la intervención legislativa. La evaluación del nivel de riesgo de un uso determinado puede basarse en las repercusiones para las partes afectadas. Por ejemplo, el uso de aplicaciones de IA con efectos jurídicos o similares en los derechos de un particular o de una empresa; aplicaciones que presenten el riesgo de causar lesiones, la muerte, o daños materiales o inmateriales significativos; aplicaciones que produzcan efectos que las personas físicas o jurídicas no puedan evitar razonablemente.

La aplicación de los dos criterios debe garantizar que el ámbito del marco regulador se adapte a lo necesario y ofrezca seguridad jurídica. En principio, los requisitos obligatorios contemplados en el nuevo marco regulador en materia de IA deben resultar de aplicación únicamente a las aplicaciones que se consideren de elevado riesgo de conformidad con la suma de los dos criterios esbozados.

No obstante, lo anterior, también puede haber casos excepcionales en los que, debido a lo que esté en peligro, el uso de aplicaciones de IA para determinados fines se considere de elevado riesgo en sí mismo; es decir, independientemente del sector de que se trate y cuando los requisitos que se presentan más abajo sigan siendo de aplicación. Por ejemplo, cabría pensar en lo siguiente:

elaborado por Axel Voss, hecho público el 2 de noviembre de 2021, estudia seis casos que afectan a sectores críticos que pueden ser un buen punto de partida para elaborar el listado al que se refiere la Propuesta de reglamento 2020. Son los siguientes: sanidad, *green deal*[98], política exterior y seguridad, proceso democrático, competitividad y mercado de trabajo[99]. Ente ellos no se encuentran las herramientas tecnológicas aplicadas en la administración de justicia y en la práctica jurídica.

En este aspecto convendría tener en cuenta, cuando se elabore ese listado, los sectores o materias referidos en el Anexo III de la AIA[100], para evitar que se den supuestos en los que un sistema de IA de alto riesgo a tenor de la AIA quede excluido del régimen especial de responsabilidad que establece este futuro Reglamento sin que, a su vez, exista un régimen especial en el derecho nacional. Esto podría abocar a que a los daños generados por sistemas de alto riesgo que, por ejemplo, emplean machine learning, se aplicara un régimen general de la responsabilidad basado en la culpa o negligencia, lo que frente a la víctima sería una diferencia de trato jurídico poco justificable, a pesar de que se hayan seguido los estrictos controles y cumplido los requisitos necesarios

---

· En vista de su importancia para las personas y del acervo de la UE en materia de igualdad de empleo, el uso de las aplicaciones de IA en los procedimientos de contratación y en situaciones que repercutan en los derechos de los trabajadores debe considerarse siempre de «riesgo elevado» y, por consiguiente, los requisitos que se presentan a continuación han de ser aplicables en todos los casos. También pueden considerarse otras aplicaciones específicas con repercusiones en los derechos de los consumidores.

El uso de aplicaciones de IA para la identificación biométrica remota y otras tecnologías de vigilancia intrusiva deben considerarse siempre de «riesgo elevado» y, por tanto, los requisitos que se presentan a continuación deben resultar de aplicación en todos los casos.

98 De muy recomendable lectura es el libro de Jeremy Rifkin, *The Green New Deal*, St. Martin's Press, New York, 2019.

99 Axel Voss, *Draft Report on artificial intelligence in a digital age*, 2020/2266 (INI), Special Committee on artificial intelligence in a digital age, 2.11.2021, p. 53.

100 Estos ámbitos son ocho: 1) Identificación biométrica y categorización de personas físicas; 2) Gestión y funcionamiento de infraestructuras esenciales; 3) Educación y formación profesional; 4) Empleo, gestión de los trabajadores y acceso al autoempleo; 5) Acceso y disfrute de servicios públicos y privados esenciales y sus beneficios: 6) Asuntos relacionados con la aplicación de la ley; 7) Gestión de la migración, el asilo y el control fronterizo; 8) Administración de justicia y procesos democráticos.

exigidos por la AIA para proceder a su comercialización, puesta en servicio o utilización (Capítulo 2 del Título III, arts. 8 ss AIA). Esto puede suceder en el caso de determinadas LegalTech tools dirigidas a los consumidores que emplean el machine learning (v. gr. procesamiento del lenguaje natural) que, a pesar de haber seguido los requerimientos que al respecto exige la AIA, los perfilan y segmentan ocasionando discriminaciones invisibles que causan un daño moral que, como tal, no será resarcido de acuerdo con el régimen de responsabilidad de la Propuesta para los sistemas de alto riesgo, ni siquiera para los de bajo riesgo. Este tipo de daños que derivan de la afectación a derechos fundamentales deberían ser considerados de alto riesgo. Y el daño moral debería compensarse con arreglo al régimen propuesto para este tipo de sistemas.

Por su parte, la AIA diferencia niveles de riesgo. En efecto, la AIA distingue entre aquellas *prácticas que están prohibidas* (art. 5 AIA) pues crean un riesgo inaceptable ya que representan una amenaza para la seguridad, la vida y los derechos de los individuos [101], los *sistemas de alto riesgo* que deben cumplir unos requisitos obligatorios *ex ante* y *ex post* comercialización o puesta en servicio (arts. 8 ss AIA), *riesgo limitado*, para los cuales establece obligaciones de transparencia que permitan a las personas conocer que está interactuando con un sistema de IA (art. 52 AIA) y *riesgo mínimo o residual* referido al resto de sistemas de IA que pueden fabricarse de acuerdo con la normativa ya existente, aunque los fabricantes pueden acogerse voluntariamente a la AIA, en cuanto a la aplicación de los requisitos señalados para los sistemas de alto riesgo, al adherirse a códigos de conducta para una IA confiable,

[101] Consistentes, a tenor del texto de compromiso hecho público el 29 de noviembre de 2021, en distorsionar el comportamiento de una persona de manera que le cause un daño físico o psicológico o a otra persona (art. 5 letra a), explotar vulnerabilidades de grupos específicos por razón de la edad, discapacidad o situación social o económica con la finalidad de distorsionar su comportamiento provocando a una persona que pertenece a ese grupo o a otro un daño físico o psíquico (art. 5 letra b), *social scoring* ya lo lleven a cabo las autoridades públicas como los particulares (art. 5 letra c), identificación biométrica en tiempo real llevada a cabo por las autoridades o en su representación, salvo que sea estrictamente necesaria en determinadas circunstancias (art. 5 letra d).

que los contemplen, elaborados por ellos o por las organizaciones a las que pertenecen (art. 69 AIA).

Además, deberá tenerse en cuenta la finalidad que persiga el sistema de IA. A estos efectos se diferencia entre una «finalidad general» (*general purpose*) o una «finalidad específica» (*intended purpose*). La primera comprende sistemas de IA que son capaces de ejecutar funciones generales como, por ejemplo, reconocimiento de voz o de imagen, detección de patrones, generación de videos, traducciones, preguntas y respuestas, etc. tal como establece el considerando núm. 70a añadido por el texto de compromiso de 29 de noviembre de 2021. En cambio, la segunda, va referida a sistemas de IA que tienen un uso específico concretado por el proveedor o por quien lo introduzca o lo ponga en servicio o en uso en el mercado incluyendo las condiciones de uso, las circunstancias para éste, dando instrucciones, etc. Esta distinción es relevante en la medida en que si el sistema de IA persigue una finalidad general no deberá cumplir los requisitos establecidos en la AIA mientras que sí serán de obligado cumplimiento en caso de una finalidad específica (nuevo art. 52a). De los supuestos indicados se puede deducir que parece pensarse en sistemas de IA de bajo riesgo o riesgo residual. Me resulta harto cuestionable que un sistema de alto riesgo que persiga una finalidad general no deba cumplir con los requisitos establecidos para éstos por la AIA. En definitiva, la relación entre el tipo de sistema de IA por el riesgo que produce y la finalidad del mismo no queda demasiado clara. En cualquier caso, si se duda si un sistema de IA es o no de alto riesgo, bastará que el fabricante indique que el sistema pone en riesgo derechos fundamentales para que sea considerado de alto riesgo y deba cumplir con los requisitos pertinentes.

En el caso de los sistemas de IA de alto riesgo, debe advertirse que la AIA contempla, por un lado, los sistemas de IA que son componentes de seguridad de otros bienes y, por otro lado, los sistemas de IA en sí mismos considerados; también conocidos como *stand-alone-AI systems*. Para que un sistema de IA sea considerado de «alto riesgo» tiene que cumplir con tres condiciones:

1. el sistema tiene que estar cubierto por la legislación que se pretende armonizar con la nueva propuesta (el ya referido «New Legislative Framework») cuyo listado aparece en el Anexo II;

2. el sistema requiera la conformidad por un tercero antes de introducirse o ponerlo en servicio en el mercado de acuerdo con la legislación que se pretende armonizar.
3. Por su parte, el art. 6.3 AIA[102] advierte que, adicionalmente, estos sistemas de alto riesgo deben de aplicarse en unos ámbitos determinados que se mencionan en el Anexo III[103].

La AIA advierte que la clasificación del riesgo que establece no tiene porqué coincidir con la clasificación del riesgo que hagan otras normas como, por ejemplo, el Reglamento (UE) de productos sanitarios, el cual clasifica los productos sanitarios según su riesgo sea de clase I, IIa, IIb, III, lo que se correspondería con riesgo bajo, riesgo medio bajo, riesgo medio alto, riesgo alto, respectivamente. Lo mismo acaece en el caso que me ocupa, pues, las condiciones que se tienen que dar para que un sistema de IA sea de alto riesgo, a tenor de la AIA, no son las mismas que se exigen en materia de responsabilidad civil, si bien, existirá a buen seguro un grueso de los sistemas de IA, que se comercialicen o se pongan en servicio como de alto riesgo, que caerán en el ámbito de aplicación de la normativa sobre responsabilidad civil porque también serán considerados conforme a ésta como de «alto riesgo». Cierta armonización de niveles de riesgo en la UE sería beneficioso para todos, pero, especialmente, para los causantes de daños, las víctimas y sus aseguradoras.

[102] El tenor del art. 6 AIA ha sido modificado por el texto de compromiso de 29.11.2021 que, ahora, queda mejor redactado. En efecto, en él se advierte que:

1. An AI system that is itself a product covered by the Union harmonization legislation listed in Annex II shall be considered as high risk if it is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the above mentioned legisation.
2. An AI system intended to be used as a safety component of a product covered by the legislation referred to in paragraph 1 shall be considered as high risk if it is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to above mentioned legislation. This provision shall apply irrespective of whether the AI system is placed on the market or put into service independently from the product.
3. AI systems referred to in Annex III shall be considered high-risk.

[103] *Vid.* nota núm. 100.

Ni en la AIA ni en la Propuesta de reglamento 2020 existe una norma en la que se contemplen los sistemas de IA de riesgo mixto, es decir, que comprendan funcionalidades propias de un sistema de alto riesgo con otras de bajo riesgo [104], ¿qué requisitos deben cumplir en este caso los sistemas de IA? ¿los propios de ambos tipos de sistemas o tan solo los de los sistemas de alto riesgo por ser más exigentes? Estas cuestiones, además de importar a efectos de las obligaciones pre y post-comercialización del sistema, son especialmente pertinentes en materia de responsabilidad civil, pues, para la víctima determinar si la funcionalidad es la propia de uno u otro sistema no va a ser especialmente fácil. En el caso de finalidades mixtas (generales con específicas) sí que existe solución al respecto pues el nuevo art. 52a apartado 3 considera que el sistema de IA estará sometido a la regulación de la AIA.

Uno de los factores esenciales, sino «el» factor esencial, para considerar a un sistema de IA como de alto o bajo riesgo es el grado de autonomía en su actuación a partir de la toma de decisiones [105]. La Propuesta de reglamento de 2020 define «autónomo» como «todo sistema de inteligencia artificial que funciona 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 asignado y otras decisiones pertinentes de diseño tomadas por su desarrollador» (art. 3 letra b). La Propuesta no establece la existencia de niveles o grados de autonomía concretos, lo que, en cambio, en materia de vehículos a motor, sí que se ha dado [106]. En efecto, se diferencian seis niveles desde el 0 al 5 considerándose que los niveles 3 y 4-5 serían los definidos como semiautónomos y autónomos respectivamente [107]. En el caso de los drones, se diferencia

[104] European Parliament, AIDA special committee, «Identification and assessment of the of existing and draft EU legislation in the digital field», p. 58.

[105] Gerhard Wagner, «Haftung für Künstliche Intelligenz», p. 551.

[106] *Vid.* la Society of Automotive Engineers, *Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems* de 2014 (J3016_201401). Accesible en: <https://www.sae.org/standards/content/j3016_201401/>. Fecha de la consulta: mayo 2022.

[107] Jesús Alberto Valero-Matas / Angie de la Barrera, «El coche autónomo, ¿un futuro mejor?», *Sociología y Tecnociencia*, 10.1 (2020): 136-158.

entre el dron pilotado desde tierra y el dron completamente autónomo pasando por una zona gris en la que el dron a pesar de ser pilotado por un humano tiene autonomía para realizar determinadas actuaciones más allá del control de aquel [108]. Esta clasificación según los grados de autonomía es importante a efectos de determinar la responsabilidad civil por los daños que ocasionen [109] y, en particular, dónde situarla en el CC mientras no se establezca una regulación comunitaria uniforme. Además, el grado de autonomía lleva a plantearse otra cuestión, cual es la de si el sistema de IA puede ser titular de derechos y/o eventualmente de obligaciones. Los diferentes niveles de autonomía del sistema tienen reflejo necesariamente en el régimen de responsabilidad civil al que se someta el operador [110]. De ello me ocuparé más adelante.

Quizá se pretende dejar la determinación del grado de autonomía a las organizaciones que establecen los estándares técnicos en la medida en que éstos devienen un elemento esencial en la regulación de los sistemas de IA. En mi opinión, concretar grados de autonomía es una tarea propia del legislador mientras que las técnicas aplicables a cada grado son las que eventualmente ser objeto de estandarización [111]. En caso contrario se corre el riesgo de conceder un excesivo poder normativo a estas organizaciones en detrimento del debate y control parlamentario.

[108] Commission delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (L 152/1, 11.06.2019), Commission implementing regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (L 152/45, 11.06.2019).

[109] Curtis E. A. Karnow, «The application of the traditional tort», pp. 57-58.

[110] Yolanda Bustos Moreno, «La irrupción de los drones (sistemas de aeronaves no tripuladas, UAS) y la responsabilidad civil. El futuro de los UAS autónomos», en *Cuestiones clásicas y actuales del Derecho de daños: Estudios en Homenaje al Profesor Dr. Roca Guillamón*, por Joaquín Ataz López y José Antonio Cobacho Gómez (coord.), Aranzadi, Thomson Reuters, Cizur Menor, 2021, pp. 889-950.

[111] Crítico con este aspecto, *vid.* Martin Ebers *et al.*, «The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)», *Multidisciplinary Scientific Journal,* 2021, 4, 589-603. <https://doi.org/10.3390/j4040043>.

2. Mal funcionamiento del sistema de inteligencia artificial

En softwares predeterminados (*locked softwares*), estandarizados y que se comercializan masivamente la determinación de un defecto no ofrece particulares dificultades, ya que se puede de forma relativamente fácil concretar, por ejemplo, aquella línea del código que se ha mal diseñado o el programa presenta una vulnerabilidad anormal a un determinado tipo de virus o de hackers. En estos supuestos, se puede conocer que el resultado del programa de ordenador no se corresponde con el resultado que se esperaba de él a partir de los datos que se suministraron. También puede ser que la información e instrucciones que acompañaban al programa de ordenador no fueran precisas o bien faltara algún dato relevante para su perfecto funcionamiento. Se podría incluso afirmar que, en estos casos, el defecto es casi obvio.

Sin embargo, la cuestión no es tan evidente en relación con aquellos sistemas de IA más complejos que, además, pueden ostentar capacidad de aprendizaje, que se adaptan a su entorno actuando autónomamente o interactuando con él emitiendo y recibiendo un constante flujo de datos o que pueden considerarse un servicio. La causa o las causas del mal funcionamiento puede estar en el algoritmo elegido, los parámetros utilizados, los pesos atribuidos a cada variable, los datos con los que se ha entrenado el sistema que son de baja calidad o existe poca variedad y volumen [112], existencia de defectos en el preprocesado de datos con duplicaciones o generalizaciones, no se han eliminado muestras de datos erróneas o incompletas, etc. La ingeniería inversa del producto obtenido lícitamente puede ser una forma de obtener información [113]. En este sentido, la Directiva 2009/24/CE, de 23 de abril, sobre protección jurídica de los programas de ordenador [114] establece en su art. 5.3 (art. 100.5 LPI) que no constituye infracción de los derechos de autor, la observación,

[112] Resolución del Parlamento europeo «Derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial», núm. 17, de 20 de octubre de 2020, 2020/2015(INI). Online: <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_ES.pdf>. Fecha de la consulta: mayo 2022.

[113] Begoña González Otero, *Interoperabilidad, Internet de las Cosas y Derecho de autor,* Madrid, Reus, 2019, pp. 57-58.

[114] DOUE L 111/16, de 5.5.2009.

estudio o verificación de su funcionamiento con el fin de determinar las ideas y principios implícitos. Esta excepción no es derogable por contrato.

Ahora bien, en aquellos sistemas de IA, respecto de los cuales no se puede saber qué causó exactamente su mal funcionamiento a la vista de los daños ocasionados *¿Cómo poder determinarlo?* En estos casos, se han propuesto algunos estándares de comparación que ayuden a dar una posible respuesta a este interrogante, si bien los resultados a los que lleguen estos estándares no son nada concluyentes y presentan un grado de ambigüedad demasiado elevado.

El primer estándar supondría comparar el programa informático a un humano, es decir, al comportamiento de un hombre razonable. Este ha sido el estándar empleado por la *US Drugs and Food Administration* (FDA) para permitir la puesta en circulación en el mercado de sofisticados programas informáticos en el ámbito de los productos sanitarios [115]. De todos modos, si la comparación pudiera funcionar cuando el sistema de IA comete el mismo tipo de errores que el humano no serviría para determinar el carácter defectuoso del sistema en caso de que éste cometiera menos errores que un humano, porque eso implicaría que el sistema de IA es «mejor» que el humano y, entonces, no tendría sentido acoger como elemento de comparación un estándar claramente inferior. Por tanto, debe establecerse un estándar más exigente para valorar el comportamiento de la máquina [116].

El segundo estándar de referencia sería ver cómo se comporta un sistema de IA similar, para comprobar si comete el mismo tipo de errores y, aquí, se puede partir de un resultado concreto o de los resultados en general que produce ese sistema. En el primer caso, esto es, comparando los sistemas en relación con un resultado específico en la misma situación, acaece que, aunque los dos estén diseñados para ejecutar las mismas tareas, pueden hacerlo

[115] Xiaoxuan Liu *et al.,* «A comparison of deep learning performance against health-care professionals in detecting diseases from Medical imaging: a systemic review and meta-analysis», *The Lancet Digital Health*, vol. 1 Octubre 2019, pp. 271-297.

[116] Gunther Teubner, «Digitale Rechssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten», *AcP*, 218/2018, pp. 164-165; Francesco Paolo Patti, «Machine Learning and European Contract Law», en André Janssen / Hans Schulte-Nölke (eds.), *Researches in European Private Law and Beyond. Contribution in Honour of Reiner Schulze's Seventieth Birthday*, Nomos Verlag, Baden-Baden, 2020, p. 119.

empleando un tipo de lógica computacional diferente, abordando la misma situación a través de dos vías diferentes. En consecuencia, es harto difícil determinar, mediante este tipo de comparación, si ha existido un error que signifique la existencia de un defecto. Por lo tanto, pareciera que la comparación de los resultados generales obtenidos por dos sistemas de IA en la misma situación, de suerte que los resultados de uno no fueran tan buenos como los del otro, podría ayudar a determinar la existencia de un defecto. El problema es que, a veces, que un sistema de IA no sea tan bueno como otro, es solo cuestión de implementar una actualización o mejora. Por lo tanto, eso no debería significar que fuera defectuoso aquel sistema de IA que no consigue tan buenos resultados por la ausencia de tal *update* o *upgrade*; en caso contrario, todos los sistemas de IA que no incorporaran la actualización o mejora serían considerados defectuosos, lo que no parece que tenga demasiado sentido [117]. Una posible solución sería considerar que el sistema de IA que se desviara en un determinado porcentaje respecto del promedio de resultados obtenidos por otros sistemas de IA equiparables [118] funcione correctamente, o comparar los resultados obtenidos por varios sistemas cuando se pretenden alcanzar finalidades generales, lo cual resulta difícil de concretar [119]. De todos modos, esto permitiría plantearse otras cuestiones tales como qué porcentaje es el adecuado [120] para considerar que un sistema de IA funciona incorrectamente y en qué fase se localiza el defecto, ¿en el diseño o en alguna de las subfases en las que se puede dividir el proceso de fabricación propiamente dicha?. Una aproximación a una posible respuesta a estas preguntas puede venir del registro del comportamiento del sistema de IA («datos»), si bien su funcionamiento, a veces, opaco no contribuirá especialmente a la determinación del defecto.

[117] Jean-Sébastien Borghetti, «How can Artificial Intelligence be Defective?», pp. 68-71; Gerhard Wagner, «Produkthaftung», pp. 735-737.

[118] Jean-Sébastien Borghetti, «How can Artificial Intelligence be Defective?2, pp. 66 ss; Gerhard Wagner, «Robot Liability», p. 44; Gerhard Wagner, «Produkthaftung», pp. 726 ss.

[119] Jean-Sébastien Borghetti, «How can Artificial Intelligence be Defective?», pp. 68-71.

[120] Ruth Janal, «Extra-Contractual Liability for Wrongs Committed by Autonomous Systems», en Martin Ebers, / Susana Navas, *Algorithms and Law*, Cambridge University Press, 2020, pp. 190-192.

3. Regímenes de responsabilidad para el «operador» o los «operadores» del sistema de inteligencia artificial

En punto a este aspecto, centraré mi atención en algunos extremos que considero de especial interés. En primer lugar, el sujeto responsable (3.1.), en segundo lugar, los dos regímenes de responsabilidad que se pretenden establecer en función del riesgo que genere el sistema de IA empezando por el atribuido a los sistemas de alto riesgo (3.2.) y siguiendo por el propio de los sistemas de bajo riesgo (3.3.).

3.1. *La figura del* «operador» *como sujeto responsable. Solidaridad*

La Propuesta de reglamento 2020 sugiere, para los sistemas de alto riesgo, una regulación del régimen de la responsabilidad basado precisamente en el riesgo para las personas y las cosas que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA pueda conllevar.

Este nuevo marco regulatorio parte, como ya he puesto de relieve, de la «gestión del riesgo» [121] o, con palabras empleadas por el *Expert Group on Liability and New Technologies* (NTF), en su Informe, con las del *Libro Blanco en IA* y con las de la Propuesta de reglamento 2020, parte de un «enfoque basado en el riesgo» para que la persona (el «operador»), que está en mejor posición para controlar y minimizar el riesgo sea quien asuma la responsabilidad por los daños que la tecnología pueda ocasionar. Este nuevo sujeto responsable (el «operador» del sistema de IA) se suma a otros sujetos responsables como el fabricante del sistema de IA, el propietario o poseedor y el usuario del mismo pudiendo eventualmente coincidir estas condiciones *in testa* de un mismo sujeto.

La Propuesta de reglamento 2020, siguiendo el Informe del *Expert Group on Liability and New Technologies* (NTF), establece que podrían ser dos o más los «operadores» del sistema de IA [122]. En particular:

[121] EU Parliament Resolution on 16 February 2017 and «Building a European Data Economy», 10.1.2017 COM(2017), 9 final.

[122] Gerhard Wagner, «Haftung für Künstliche Intelligenz», p. 553.

a. la persona que principalmente decide y se beneficia del uso de la tecnología (*frontend operator* u *operador inicial,* art. 3 letra e Propuesta de reglamento 2020), que podría ser el propietario, el poseedor o un simple usuario del sistema de IA; y
b. la persona que define continuamente las características de la tecnología y proporciona soporte esencial y continuo como, por ejemplo, datos, ejerciendo un grado de control asociado al funcionamiento del sistema (*backend operator* u *operador final*[123], art. 3 letra f Propuesta de reglamento 2020) como serían el desarrollador, el diseñador, el fabricante del sistema de IA.

Fundamental, pues, para ser considerado sujeto responsable, es el «grado de control» que se tenga sobre el sistema de IA. A estos efectos, la Propuesta de reglamento 2020 entiende como «control»: «toda acción de un operador que influya en el funcionamiento de un sistema de IA y, por consiguiente, la medida en que el operador expone a terceros a los potenciales riesgos asociados a la operación y al funcionamiento del sistema de IA; esa acción puede afectar al funcionamiento en cualquier fase al determinar la entrada, la salida o resultados o pueden cambiar funciones o procesos específicos dentro del sistema de IA; el grado en que estos aspectos del funcionamiento del sistema de IA están determinados por la acción depende del nivel de influencia que el operador tenga sobre el riesgo relacionado con la operación y el funcionamiento del sistema de IA» (art. 3 letra g).

Otra cuestión es si responden solidariamente o de manera proporcional[124]. La responsabilidad solidaria es vista como la mejor solución por el *Expert Group on Liability and New Technologies* (NTF) en su informe referido[125] y es la establecida en la Propuesta de reglamento 2020 (art. 11), sin perjuicio

[123] Pilar Álvarez Olalla considera que la traducción española de los términos ingleses de «frontend operator» y «backend operator» está invertida en la medida en que el inicial debería ser el final y viceversa («Propuesta de reglamento en materia de responsabilidad civil por el uso de inteligencia artificial, del Parlamento europeo, de 20 de octubre de 2020», *Revista CESCO de Derecho de Consumo*, núm. 37/2021, pp. 3-4).

[124] Respecto a la responsabilidad proporcional, *vid.* Capítulo II.

[125] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 57-58.

de las acciones de regreso del que satisfizo la indemnización a la persona afectada frente a los otros corresponsables (art. 12) en el régimen especial de responsabilidad en materia de IA. En relación con las acciones de regreso, el art. 12 establece un requisito adicional para su ejercicio entre los operadores, cual es, que el operador que la ejercita haya abonado a la víctima la totalidad de la indemnización a que tenga derecho. Eso si consigue saber quienes son, lo cual no es, en un entorno complejo de máquinas inteligentes interconectadas, nada fácil. En ambos regímenes de responsabilidad considerados por la Propuesta de reglamento, la regla del reparto entre los operadores en vía de regreso será la proporcionalidad en función de los niveles de riesgo que estén bajo su control. Se establece la solidaridad de los operadores en vía de regreso en caso de que uno de ellos fuera insolvente, por su parte proporcional frente al operador que abonó la totalidad de la indemnización. Igualmente, se establece una acción de regreso del operador que abonó toda la indemnización frente al fabricante cuando el daño haya sido causado por un defecto del sistema de IA [126].

Llama la atención la ausencia de una norma que recoja la responsabilidad vicaria del empresario por los hechos de sus auxiliares cuando éstos son sistemas de IA semiautónomos y autónomos en sustitución de auxiliares humanos [127], a la cual, sin embargo, sí hace referencia el *Expert Group on Liability and New Technologies* en su Informe (recomendaciones núms. 18-19) [128].

3.2. *Régimen de responsabilidad objetiva para los sistemas de alto riesgo*

En primer lugar, me centraré en los sistemas de IA semiautónomos (3.2.1.) y seguidamente en los autónomos (3.2.2.). A continuación, destacaré los daños cubiertos por este nuevo régimen de responsabilidad (3.2.3.) y los plazos establecidos para las pretensiones que se deriven (3.2.4.).

[126] Pilar Álvarez Olalla, «Propuesta de reglamento», pp. 9-10.

[127] Christiane Wendehorst, *Safety and Liability Related Aspects of Software*, p. 96.

[128] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 45-46.

Desde el derecho español vigente de la responsabilidad civil debe preguntarse por la solución legal cuando un sistema de alto riesgo, es decir, sistemas de IA semiautónomos y autónomos, provoca daños. De entrada, debe dejarse clara la diferencia entre uno y otro. En el primero, la persona puede y/o debe tomar el control del sistema de IA cuando lo considere oportuno o cuando el propio sistema lo requiera. La persona, por tanto, puede ejercer una determinada influencia sobre el sistema (*human-over-the-loop*). En cambio, en el segundo, la persona no ejerce ninguna influencia, no toma el control del sistema ni puede tomar decisión alguna. El sistema toma las decisiones a partir de su algoritmo de referencia, de la información que procesa en cada momento sin que se puedan revertir aquellas por el humano (*human-out-of-the-loop*) [129]. Ambos sistemas de IA caerán en el ámbito de aplicación del régimen jurídico de la responsabilidad objetiva conforme a lo previsto en la Propuesta de reglamento 2020, si bien los sistemas de IA completamente autónomos no parecen, a tenor de la AIA, que se vaya a permitir, al menos de momento, su comercialización, puesta en servicio o utilización, pues la AIA requiere siempre y, en todo caso, la supervisión humana (art. 14.1: «Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cosas»). A pesar de ello, y aunque solo sea a efectos de imaginar hipótesis que, aunque en la actualidad no se contemplan, quizá acaben existiendo y contemplándose en un futuro, me parece necesario diferenciar entre unos y otros porque las soluciones legales vigentes, en las que me centro seguidamente, no serían necesariamente las mismas.

3.2.1. *Sistemas de inteligencia artificial semiautónomos. Aplicación analógica de los arts. 1903.4 o 1905 CC*

En el caso de sistemas de IA semiautónomos que ocasionan daños, me parece que la aplicación por analogía de la regla establecida en el art. 1905 CC

[129] Simon Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law*, Cambridge University Press, Cambridge, 2021, pp. 85 ss.

en caso de responsabilidad civil por los daños ocasionados por los animales podría ser la solución [130]. En ambos casos, existe un grado de autonomía que no impide que el poseedor ejerza su influencia en el comportamiento del animal; en nuestro caso, del sistema de IA. Además, permite contemplar como responsables al «poseedor» o al que «se sirve de él», lo que comprende tanto al sistema de IA corpóreo (*embebed AI*) como al intangible (*stand-alone-AI system*). Aplicada la norma a éste permite entender comprendidos tanto al operador «inicial» como al «final». Solución ésta que más difícilmente se puede encontrar en el art. 1908 CC cuando alude a la «explosión de la máquina» de la que se hace responsable a su «propietario», si ocasiona algún daño, salvo que se fuerce en demasía el tenor literal del precepto.

Otra posible solución sería aplicar la responsabilidad vicaria del empresario recogida en el art. 1903.4 CC que expongo seguidamente para los sistemas autónomos. En efecto, ambos sistemas de IA —semiautónomos y autónomos— tienen características muy similares en cuanto a capacidad de aprendizaje y toma de decisiones exceptuando que sobre el comportamiento de los autónomos no existe supervisión humana, cosa que no acontece en el caso de los semiautónomos. Sin embargo, ambos pueden caer bajo el mismo régimen jurídico en aras a una mayor protección de las víctimas, amén de no complicar en exceso el derecho de la responsabilidad civil con distinciones que poco aportan desde el punto de vista de los efectos jurídicos y de la práctica.

[130] Susana Navas Navarro, «Smart robots y otras máquinas inteligentes en nuestra vida cotidiana», *Revista CESCO de Derecho de Consumo*, núm. 20/2016, pp. 82-109; Ángel F. Carrasco Perera, «A propósito de un trabajo de Gunther Teubner sobre la personificación civil de los agentes de inteligencia artificial avanzada», *Centro de estudios de Consumo,* publicaciones jurídicas, <http://centrodeestudiosdeconsumo.com>. Fecha de la consulta: mayo 2022; Silvia Díaz Alabart, *Robots y responsabilidad civil*, Reus, Madrid, 2018, *in totum*; Guillermo Cerdeira Bravo de Mansilla, «Entre personas y cosas: animales y robots», *Actualidad Jurídica Iberoamericana*, núm.14, febrero 2021, pp. 14-53; Miguel L. Lacruz Mantecón, «Robots y responsabilidad civil», en Carlos Rogel Vide (coord.), *Los robots y el Derecho*, Reus, Madrid, 2018, pp. 99-114; Juan Gómez-Riesco Tabernero de Paz, «Los robots y la responsabilidad civil extracontractual», en Moisés Barrio Andrés (dir.), *Derecho de los robots*, Wolters Kluwer, La Ley, Madrid, 2018, p. 118.

3.2.2. *Sistemas de inteligencia artificial autónomos*

Si el sistema de IA es completamente autónomo sin posibilidad de influencia humana, se plantea, entonces, en primer lugar, si ese sistema puede ser «sujeto de derecho» (A.) y, en segundo término, qué régimen de responsabilidad civil de los vigentes se podría aplicar por analogía (B.).

A. *Su consideración como* «sujeto de derecho»

El Derecho es antropocéntrico. Siempre ha girado alrededor del ser humano. Está hecho por y para el ser humano. Es él el único al que se atribuye personalidad jurídica, por el hecho de nacer (arts. 29-30 CC), lo que implica convertirse en sujeto de derecho. Existe una excepción, como es conocido, cuando se trata de la consecución de unos mismos fines por varios individuos, en cuyo caso pueden actuar como si fueran uno solo mediante la constitución de una persona jurídica (art. 35 CC). Es la primera abstracción (ficción) legal de la persona [131]. Sin embargo, también existen patrimonios sin titular afectos a una finalidad a los que se aplica esta ficción legal, es decir, que se finja que son una «persona» pero «jurídica», para actuar en el tráfico jurídico como un único sujeto. Es el caso, por ejemplo, de las fundaciones que persiguen finalidades de interés general (art. 35.1 CC).

Desde el siglo XIX, a partir sobre todo de F. C. v. Savigny [132], se ha venido atribuyendo a la persona, en la medida en que por el mero hecho del nacimiento adquiere personalidad jurídica, como decía, la condición de sujeto de derecho [133]. Desde entonces no se ha revisado este planteamiento. Parece que, como paso previo, a ser sujeto de derecho es la necesidad de que se le atribuya personalidad jurídica. Así, sin personalidad jurídica no se puede ser sujeto de

[131] Ngaire Naffine, «Legal Persons as Abstractions: The Extrapolation of Persons from the Male Case», en Visa A. J. Kurki, Thomasz Pietrykowski (eds.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Springer, 2017, p. 16.

[132] Friedrich Carl von Savigny, *System des heutigen Römischen rechts*, Veit ,1840, § 60.

[133] Visa A. J. Kurki, «Why Things Can Hold Rights: Reconceptualizing the Legal Persons», en Visa A. J. Kurki / Thomasz Pietrykowski (eds.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Springer, 2017, pp. 71-74. Del mismo autor, *vid.* Visa A. J. Kurki, *A theory of legal personhood*, Oxford University Press, 2019, pp. 36 ss.

derecho ya que la condición para ser sujeto de derecho es ser «persona». Por eso, al situar en el centro a la persona física o natural, los grupos de personas o los patrimonios, para poder ser sujetos de derechos, deben emular a aquélla y eso se hace atribuyéndoles «personalidad jurídica».

La atribución de personalidad jurídica va fuertemente vinculada a la idea de «persona física». Por ello, en otros supuestos debe «fingirse» que lo son mediante la atribución de personalidad jurídica. Se convierten en «personas» pero «jurídicas». Esto supone que para que entidades diferentes al ser humano puedan llegar a ser sujetos de derecho, se les debe atribuir mediante ley, como paso previo, personalidad jurídica. Sin la atribución legal de personalidad jurídica no se puede ser sujeto de derecho. Esto es así en la medida en que se pretende imitar o emular a la persona física. Precisamente, ello ha supuesto un obstáculo para que otras entidades o seres sintientes puedan llegar a convertirse en sujetos de derechos puesto que no se les atribuye personalidad jurídica al no considerarse equiparables al ser humano. Ahora bien, que la consecuencia de la atribución de personalidad jurídica sea el convertirse en sujeto de derecho, no debería llevar necesariamente a que sea cierta la proposición contraria; a saber, que, para ser sujeto de derecho, se tenga que atribuir previa y necesariamente personalidad jurídica.

Este es otro de los conceptos jurídicos que más están notando el efecto disruptivo que provoca la tecnología inteligente y que requerirá, aunque en la actualidad se dude mucho al respecto, una solución legal también disruptiva. En este trabajo propongo que en la medida en que la atribución de «sujeto de derecho» es una atribución que hace la ley, es pensable que se pueda asignar esa condición a un ente no-persona como, por ejemplo, a los animales (arg. ex nuevo art. 333 bis.1 CC: «Los animales son seres vivos dotados de sensibilidad»; art. 511-1.3 CCCat: «Los animales, que no se consideran cosas, …») [134], sin necesidad de atribuirle primero y, en todo caso, personalidad jurídica.

En esta línea de pensamiento, si se deja de atribuir necesariamente personalidad jurídica para poder ser sujeto de derecho entendiendo que, si bien

[134] Thomasz Pietrykowski, «The Idea of Non-Personal Subjects of Law», en Visa A. J. Kurki / Thomasz Pietrykowski (eds.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Springer, 2017, pp. 60-63.

toda persona física tiene personalidad jurídica desde su nacimiento y de ahí que sea sujeto de derecho, no todo sujeto de derecho ha de ser una persona o ha de atribuírsele personalidad jurídica para poder serlo, se abre el abanico de posibilidades para que otros seres o entidades no se vean privados de ser «sujeto de derecho». La atribución de personalidad jurídica representa, en estos casos, un obstáculo debido a su difícil equiparación a la persona humana. Admitir este planteamiento, llevaría a reconsiderar la ficción legal respecto de los patrimonios sin titular en el sentido de que podrían ser sujetos de derecho sin tener necesariamente que atribuírseles personalidad jurídica. De hecho, el estatuto jurídico del «sujeto de derecho-no persona» debería definirse y delimitarse en cada caso concreto. Así, en algunos casos, se atribuiría un solo derecho; en otros, varios; en otros, además de derechos, se atribuirían obligaciones [135].

Sin asumir todavía que los vegetales y la naturaleza [136], también seres sintientes, pueden merecer la consideración de titulares de derechos, se ha venido planteando la atribución de personalidad a los sistemas de inteligencia artificial (en adelante, IA), la denominada «personalidad electrónica» [137], que, al menos de momento, se ha descartado al partir del discurso de que solo los seres humanos tienen personalidad y que, por tanto, a un sistema de IA por mucho que exhiba capacidades similares al humano, incluso que físicamente se asemeje a él, como en el caso de los denominados robots asistenciales (*embodied* AI), no se le puede atribuir tal personalidad.

Ahora bien, si se deja de pensar en clave «ser humano=personalidad jurídica=sujeto de derecho» y se piensa en clave «ser humano/no-ser

[135] Luz Sánchez García, *El inventor artificial. Un reto para el Derecho de Patentes*, Aranzadi, Thomson Reuters, Cizur Menor, 2020, pp. 94-94. La autora define al agente artificial como «centro de imputación de actuaciones». Por su parte, Gunther Teubner plantea la posibilidad de reconocer a los agentes artificiales una subjetividad jurídica parcial («Digitale Rechssubjekte?», pp. 162-163).

[136] «Towards an EU Charter of the Fundamental Rights of Nature», estudio encargado por el Comité europeo económico y social (diciembre, 2019). Online: <https://www.eesc.europa.eu/sites/default/files/files/qe-03-20-586-en-n.pdf>. Fecha de la consulta: mayo 2022.

[137] Gerald Spindler, „Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?«, *CR* 12/2015, pp. 774-775.

humano=sujeto de derecho» podría aceptarse la atribución a un sistema de IA de la condición de «sujeto de derecho». De todos modos, en la medida en que un sistema de IA revista diferentes grados de autonomía, en función de la mayor o menor intervención humana en cuanto a su vigilancia, podría atribuirse esa calificación solo a aquellos sistemas completamente autónomos no supervisados, en los que la intervención humana se encuentra en la inicial concepción del sistema sin que se imaginen los resultados a los que conduce el funcionamiento del mismo, los cuales pueden ser el resultado del algoritmo creado por el algoritmo primigenio como en el caso de los denominados «algoritmos genéticos». Consiguientemente, la imputación objetiva de este resultado a la persona difícilmente podría establecerse sobre la base de la previsibilidad y de la teoría de la causalidad adecuada. Estos últimos tipos de sistemas son los que interesan a este trabajo. Reconocerles su condición de «sujetos de derecho» supone permitir que coexistan con los humanos, con los animales, con los vegetales y con la naturaleza. Es decir, supone que siga poniéndose en entredicho, aunque solo sea un poco, el antropocentrismo del Derecho porque se reconocería como sujetos de derecho solo a aquellos que exhibieran una autonomía «casi» idéntica a la humana [138].

Y es que en el mundo de la IA se intenta emular al cerebro humano (IA fuerte [139]) persiguiendo incluso superarlo (superinteligencia artificial [140]), cosa que no sucede en el ámbito animal ni en el vegetal. En ambos, sin embargo, los investigadores han constatado la existencia de «inteligencia» [141], diferente a la del hombre, pero, al fin y al cabo, «inteligencia» entendida ésta, de forma

[138] Visa A. J. Kurki, *A theory of legal personhood,* pp. 178 ss.

[139] La IA fuerte es la que muestra capacidades cognitivas idénticas a las del humano. Estas máquinas tendrían conciencia, emociones, y actuarían de la misma manera que lo hace un humano (Ray Kurzweil, *How to create a mind. The secret of human thought revealed*, Penguin Books, New York, 2013, *in totum*).

[140] Se refiere a aquel sistema que exhibe capacidades superiores al humano en todos los ámbitos (Nick Bostrom, *Superintelligence. Paths, Dangers, Strategies*, Oxford University Press, Oxford, 2014, *in totum*).

[141] Stefano Mancuso, *Inteligencia y sensibilidad de los vegetales,* Galaxia Gutenberg, Barcelona, 2.ª ed., 2015, p. 117; Daniel C. Dennett, *De las bacterias a Bach. La evolución de la mente*, traducción de Marc Figueras, Pasado & Presente, Barcelona, 2017, pp. 86 ss.

sencilla, como la capacidad de resolver problemas [142]. Dicho con otras palabras, se debería asumir que la inteligencia humana es una de las posibles inteligencias que pueden existir. Las máquinas que, en este contexto, se identifican con los sistemas de IA, tienen su «propia» inteligencia que no tiene porqué ser o acercarse tan siquiera a la humana. Incluso las máquinas entre ellas pueden exhibir «inteligencias» diferentes [143]. De hecho, éstas no tienen por qué asemejarse a los humanos, ni tienen por qué tener la misma inteligencia que éstos ni tienen por qué hacer cosas similares a nosotros. Son diferentes formas de inteligencia. En lugar de competir debería establecerse una suerte de colaboración con ellas. En este sentido, no necesitamos «reconstruir» al ser humano, sino entender que la visión antropocéntrica del mundo se va paulatinamente diluyendo [144] como consecuencia, en parte, pero no solo, de la disrupción tecnológica y esto provoca una disrupción legal de primer orden en la medida en que pone en cuestión el fundamento mismo en el que se asienta el Derecho.

Además, atribuirle la condición de «sujeto de derecho» permitiría en caso de responsabilidad establecer el juicio de imputabilidad con el sistema de IA mientras que el juicio de responsabilidad se establecería con humano, el cual podría ser el propietario o poseedor (especialmente, el usuario del sistema de IA) del sistema de IA. O sea, permitiría aplicar, por analogía, el esquema de la responsabilidad por hecho ajeno (arts. 1903.4 CC) [145]. En particular, la responsabilidad vicaria del empresario. A ella aludo a continuación.

[142] Los enfoques, las técnicas y las capacidades varían según a qué entidad humana o no humana nos refiramos. Sobre ello, *vid.* Mark Coeckelbergh, *Ética,* pp. 23 ss.

[143] Richard Susskind / Daniel Susskind, *El futuro de las profesiones. Cómo la tecnología transformará el trabajo de los expertos humanos*, editorial Teell, trad. por Juan Carlos Ruiz Franco, Zaragoza, 2016, pp. 263 ss.

[144] Donna Haraway, «A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century», *Simians, Cyborgs and Women. The Reinvention of Nature*, Nueva York, Routledge, 1991, pp. 149-181; Rosi Braidotti, *El conocimiento posthumano*, Gedisa, 1.ª ed., trad. por Júlia Ibarz, Barcelona, 2020, pp. 10 ss.

[145] Al respecto, *vid.* mi trabajo «Sistemas expertos basados en inteligencia artificial y responsabilidad civil», Diario La Ley, Ciberderecho, 11.12.2019. Online: <https://diariolaley.laleynext.es/dll/2019/12/13/sistemas-expertos-basados-en-inteligencia-artificial-y-responsabilidad-civil>. Fecha de la consulta: mayo 2022.

B. *La responsabilidad del* «principal» *(el humano) por los hechos de su* «auxiliar» *(el sistema de IA autónomo): art. 1903.4 CC*

Como he manifestado, en mi opinión, la atribución de la condición de «sujeto de derecho» a los sistemas de IA solo tiene la virtualidad de hacerlos «imputables» de conductas respecto de las cuales «responde» un humano. En este caso, la responsabilidad por hecho ajeno sería el fundamento de responsabilidad adecuado pues debemos tener en cuenta la actuación de dos posibles «sujetos de derecho», el humano y el sistema de IA, de suerte que la actividad o conducta de cada uno de ellos es relevante para establecer si existe responsabilidad o no.

Así, si hay un incumplimiento de los deberes de cuidado, el humano que responde por el sistema de IA lo hace porque él ha infringido un deber de conducta. Pero también requiere una «mala» actuación por parte del sistema de IA en la medida en que hace algo por lo que si lo hubiera hecho una persona hubiera tenido que responder (*principio de equivalencia funcional*). Extremo significativo, a este respecto, es el criterio o criterios a tener en cuenta para determinar cuándo una actuación de un sistema de IA es «mala» o «incorrecta», aspecto éste que se ha tratado en el apartado 2 de este capítulo.

El supuesto al que me estoy refiriendo es diferente del caso en que el sistema de IA propone una determinada actividad a realizar al humano siendo éste el que finalmente decide si se sigue lo propuesto por el sistema inteligente o lo que él mismo o un equipo de personas considere más conveniente. Si la decisión adoptada es seguir el criterio establecido por el software conllevando una serie de daños, la responsabilidad es de aquel sujeto (o sujetos) que toma la decisión final. Se trata de una responsabilidad por hecho propio; no, por hecho ajeno.

Pues bien, en el caso de sistemas de IA autónomos, la responsabilidad por hecho ajeno podría basarse en la relación existente entre el humano y el sistema pues el primero se beneficia de la actividad que lleva a cabo el segundo. En este caso, la responsabilidad de la que se suele hablar es la del «empresario» por los hechos de sus «dependientes» (art. 1903.4 CC). En realidad, la «dependencia» cubre todos aquellos casos en los que una persona o, en nuestro caso, un sistema de IA, actúa subordinada a las instrucciones de otra que sería el empresario o, como se la conoce en textos legales europeos,

el «principal», sin que se ciña al contrato de trabajo o de servicios. Por tanto, existe un «principal» (el humano) y un «auxiliar» (el sistema de IA)[146].

Ahora bien, uno de los requisitos de aplicación de la responsabilidad del principal por los hechos de los auxiliares es la relación de subordinación o dependencia en la que quién imparte las instrucciones es el principal. Sin embargo, en el caso que me ocupa, los sistemas de IA autónomos, si bien, en algunos casos, pueden tener unas instrucciones previas, en virtud de su capacidad de aprendizaje y autonomía a la hora de tomar decisiones actúan sin estar sujetos al control del principal que se beneficia de su actividad. No existe el vínculo de subordinación característico de la responsabilidad vicaria del principal por los hechos de su auxiliar. Más bien se asemejaría a la situación del contratista independiente.

De hecho, no existe verdadera identidad de razón en aquellos casos en los que el sistema de IA actúa de forma independiente a las instrucciones dadas o que partiendo de ellas después, a partir de su aprendizaje, se aleja de ellas. Sin embargo, hacer cargar al principal con las consecuencias dañosas del comportamiento del sistema de IA del que se sirve y se beneficia concuerda con la idea de que quien disfruta del beneficio que genera el sistema de IA es el principal[147]. Así, el caso paradigmático es la negociación algorítmica de alta frecuencia.

Por otro lado, que el principal asuma las consecuencias dañosas generadas por el sistema de IA sería también un incentivo para que despliegue un mayor control de los riesgos que pueden resultar de la actividad de aquél en la medida en que se encuentra en mejor posición para establecer mecanismos de prevención (v. gr. auditorías periódicas del sistema, posibles modificaciones del código fuente, seguimiento de su comportamiento o contratación de un

[146] Una solución similar propone Gunther Teubner para el derecho alemán («Digitale Rechssubjekte?», pp. 190-193).

[147] A favor de considerar las máquinas como «auxiliaries» se muestra Ernst Karner, «Liability for Robotics: Current Rules, Challenges, and the Need for Innovative Concepts», en Sebastian Lohsse / Reiner Schulze / Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Nomos Verlag, Baden-Baden, 2018, p. 120; Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, Springer, 2013, pp. 37-43.

seguro). El principal además estará en mejor posición de hacer frente a los costes tanto de la prevención como indemnizatorios (*cheapest cost avoider*). Por todas estas razones y, además, si se le considerara legalmente «imputable» mediante la atribución ya sea de «personalidad» o, sencillamente, se le incluya en la categoría de «sujeto de derechos», podría entenderse de aplicación, por analogía, aunque no existiera auténtica identidad de razón, la responsabilidad vicaria del principal por los hechos del «auxiliar» que es un sistema de IA completamente autónomo [148].

3.2.3. *Daños. Obligación de aseguramiento*

La Propuesta de reglamento 2020 recoge, en el art. 6, el alcance de la indemnización que debe abonar el operador a la víctima, la cual comprende los siguientes conceptos [149]:

a. *Daños físicos que pueden conllevar la muerte de la víctima*, cuyo cálculo se hará sobre la base de los costes del tratamiento médico que haya seguido antes de fallecer, así como el perjuicio económico sufrido antes de la muerte 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. Además, reembolsará los gastos funerarios de la persona afectada a quien los hubiera satisfecho. Si en el momento en que se ocasionó el daño, la persona afectada tenía el deber de mantener a un tercero, el operador indemnizará a ese tercero mediante el pago de una pensión alimenticia proporcional a la que la persona afectada se habría visto obligada a pagar, durante el período equivalente a la esperanza de vida media de una persona de su edad y teniendo en cuenta su estado general. También indemnizará al concebido pero no nacido. El límite máximo del importe a satisfacer por el operador será de dos millones de euros (art. 5.1 letra a).

[148] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 45-46.

[149] Los daños corporales siguen de cerca normas sobre responsabilidad civil del derecho alemán (Gerhard Wagner, «Haftung für Künstliche Intelligenz», pp. 566-567).

b. *Daños físicos que comportan una lesión a la víctima que no le ocasiona la muerte*, el operador responsable reembolsará 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 mediante un certificado médico. El importe máximo de la indemnización será de un millón de euros (art. 6.2 y art. 5.1 letra b).

c. *Daños morales significativos que resulten en una pérdida económica comprobable o en daños materiales, también cuando distintos bienes, propiedad de la persona afectada, resulten dañados como resultado de un único funcionamiento de un único sistema de IA de alto riesgo*. La indemnización no podrá superar el límite de un millón de euros (art. 5.1 letra b). Este límite es un límite conjunto con los daños físicos anteriormente aludidos en el apartado b que no podrá superar en total el millón de euros.

Por tanto, no se indemniza el daño moral en sí mismo, sino las consecuencias económicas de éste[150]. De hecho, esta norma no es extraña a la responsabilidad, pues, en un área muy cercana a esta, como es la responsabilidad del fabricante por producto defectuoso no se contempla la indemnización, en principio, del daño moral[151]. Ahora bien, los sistemas de IA se manejan con una cantidad ingente de datos, sobre todo, aquellos que tienen capacidad de aprendizaje, y los datos pueden estar no del todo depurados de manera que los resultados que se deriven estén sesgados provocando discriminaciones invisibles, valoraciones de la personalidad de un individuo que luego se traducen en comportamientos discriminatorios de terceros, pérdidas de oportunidades o la afectación de su honor y reputación. En mi opinión, deberían incluirse este

[150] Pilar Álvarez Olalla, «Propuesta de reglamento», pp. 6-7. Crítico con la ausencia de indemnización del «Schmerzgeld» se muestra Gerhard Wagner («Haftung für Künstliche Intelligenz», p. 567).

[151] Sobre ello, *vid.* mi estudio «Daño moral y producto defectuoso. Estado de la cuestión legal y jurisprudencial en España», *Revista Crítica de Derecho privado (Uruguay)*, vol. 13, 2016, pp. 525-573.

tipo de daños —también denominados «daños sociales» [152]— en el ámbito de aplicación de esta Propuesta de reglamento. En caso contrario, la víctima se ve abocada a ejercitar diferentes pretensiones basadas en daños diferentes sobre la base de legislaciones diferentes (art. 2.3. Propuesta de reglamento 2020). Téngase en cuenta que tampoco se indemnizan los daños económicamente puros (v. gr. trading de alta frecuencia). En cualquier caso, debería haber una mayor coordinación entre los riesgos de daños que tiene en cuenta la AIA a lo largo de su articulado y los daños indemnizables en el régimen especial de responsabilidad civil por los daños que ocasione un sistema de IA.

No deja de sorprender que la propuesta de reglamento no contemple como posibles daños, los ocasionados a los «datos» o a «bienes o productos digitales» como, por ejemplo, criptomonedas que la víctima tuviera almacenadas en un monedero electrónico, o a una obra digital tokenizada, que, aunque pueden eventualmente comprenderse dentro del ámbito de aplicación de la responsabilidad del fabricante en una futura revisión de la norma comunitaria a la sazón vigente, pueden también comprenderse en el ámbito de aplicación de la responsabilidad civil ya sea por que se ocasionan daños a los mismos (v. gr. deterioro, borrado, contaminación, alteración o encriptado) o a los dispositivos en los que se almacenan. No obstante, se podrían comprender en los daños materiales a bienes propiedad de la víctima pues no se especifica el tipo de bienes; por tanto, pueden ser tanto bienes tangibles como intangibles.

No me parece acertado que los daños cubiertos por este régimen especial de responsabilidad se ciñan a daños más propios del mundo analógico ocasionados por un sistema de IA, que es un bien intangible, que actúa en el mundo digital y que, en cambio, bienes intangibles de titularidad de la víctima o víctimas que pueden verse dañados por el comportamiento del sistema de IA resulten excluidos. Resulta ciertamente contradictorio. Por ello, el *Expert Group on Liability and New Technologies* recomienda (núm. 32) en su informe que se contemple el daño generado a este particular bien intangible [153], cual representan los «datos».

[152] Christiane Wendehorst, *Safety and Liability Related Aspects of Software*, p. 30.

[153] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 59-60.

Cuando existan varias víctimas por el daño ocasionado por un mismo sistema de IA, la cuantía máxima —2 o 1 millón según el caso— no se sobrepasará, sino que se repartirá entre ellas de forma proporcional al daño sufrido (art. 5 Propuesta de reglamento 2020).

Los operadores de sistemas de alto riesgo, según dispone el art. 4.4 Propuesta de reglamento 2020 siguiendo al Informe del *Expert Group on Liability and New Technologies* (NTF)[154], tienen la obligación de concertar un seguro obligatorio, ya se trate del operador inicial como del final. La cobertura de este seguro se ciñe a los topes indemnizatorios antes referidos. De todos modos, el operador inicial o *backend operator* puede optar por contratar un seguro de responsabilidad por productos o un seguro empresarial. Opción que le concede la Propuesta pensando seguramente que este operador sea, a su vez, el fabricante del sistema de IA.

3.2.4. *Plazos*

El art. 7 de la Propuesta de reglamento 2020 establece un plazo de prescripción especial de 30 años a contar desde la fecha que se produjo el daño para las pretensiones de responsabilidad civil relativas a los daños a la vida, a la salud o la integridad física de la persona afectada.

En el caso de daños materiales o daños morales considerables que resulten de una pérdida económica comprobable, se establecen plazos de prescripción especiales: 10 años cuando se produjo el menoscabo a los bienes o la pérdida económica comprobable resultante de un daño moral significativo a contar desde la fecha que se produjo el menoscabo o 30 años a contar desde la fecha en que tuvo lugar la operación del sistema de IA de alto riesgo que causó posteriormente el menoscabo a los bienes o el daño moral. De los dos plazos será aplicable el que venza antes.

Se deja a los estados miembros la regulación de la suspensión o interrupción de los plazos de prescripción en estos casos.

[154] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 61-62.

3.3. *Régimen de responsabilidad subjetiva en caso de sistemas de bajo riesgo*

En relación con los daños que pueda ocasionar la tecnología de «bajo riesgo», el régimen de responsabilidad propuesto es el subjetivo basado en la culpa o negligencia del operador (art. 8 Propuesta de reglamento 2020). Este régimen está presente en todos los ordenamientos jurídicos occidentales, si bien, el establecido por la Propuesta deja asentado que el operador deja de ser responsable cuando: a) el sistema se activara sin su consentimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador; 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 (art. 8.2).

Fuera de estos casos solo dejará de responder por causa de fuerza mayor. Así, no cabe probar el empleo de cualquier diligencia que pudiera ser exigible, sino que tendrá que probar las dos causas antes indicadas. La diligencia se graduará en función de si el operador es un profesional o un consumidor. A la vista de ello, no se trata de un régimen de responsabilidad subjetivo puro, sino más bien de un régimen de responsabilidad cuasiobjetivo o de responsabilidad subjetiva objetivizada[155].

Los plazos de prescripción en caso de daños ocasionados por sistemas de IA de bajo riesgo, así como qué daños se indemnizan y los límites máximos estarán sujetos a lo establecido en la legislación del estado miembro en el que se haya producido el daño o perjuicio económico (art. 9).

Desde el derecho vigente los daños ocasionados por sistemas de IA de bajo riesgo tendrán acomodo, en mi opinión, en la regla general del art. 1902 CC. Normalmente se producirán en una esfera privada sin que exista —o muy difícilmente— incertidumbre subjetiva acerca del causante del daño o de la víctima, aunque llegado el caso se podría aplicar la norma acerca de la responsabilidad por los daños ocasionados por «explosiones» de máquinas

[155] Pilar Álvarez Olalla, «Propuesta de reglamento», pp. 9-10.

(art. 1908.1 CC) que establece, como se conoce, un régimen de responsabilidad objetiva.

De otra parte, en la medida en que estos sistemas siguen considerándose «productos», si éstos son defectuosos, se aplicarán las normas de responsabilidad del fabricante por los daños que generen. Aquí, se plantea la divergencia entre el régimen de responsabilidad de la Propuesta de reglamento 2020 que es subjetivo, aunque objetivizado, y el régimen de la responsabilidad objetiva del fabricante por el ejercicio de una actividad anormalmente peligrosa. Si se aplican las normas de la Propuesta con carácter preferente, esto puede suponer una menor protección para la víctima en comparación con el nivel de protección que le proporciona el régimen más estricto de responsabilidad del fabricante.

Otro inconveniente que presenta esta Propuesta en relación con los sistemas de bajo riesgo guarda relación con el hecho de que el *front-end operator* u operador inicial sea una persona consumidora o, incluso, que se trate de una persona consumidora vulnerable [156] que carece de las habilidades digitales o informáticas necesarias para entender el perfecto funcionamiento del sistema y, por ejemplo, pararlo a tiempo antes de que produzca daños a terceros. La aplicación de este fundamento de responsabilidad cuasiobjetivo en lugar del tradicional por culpa de los derechos nacionales puede resultar problemático [157].

4. **La prueba. Derecho de acceso a los datos**

4.1. ***La prueba de presunciones***

La Propuesta de reglamento 2020 no prevé ninguna presunción *iuris tantum* o una regla de inversión de la carga de la prueba ya sea del nexo cau-

[156] Art. 3.2 TRLGDCU: «tienen la consideración de personas consumidoras vulnerables respecto de relaciones concretas de consumo, aquellas personas físicas que, de forma individual o colectiva, por sus características, necesidades o circunstancias personales, económicas, educativas o sociales, se encuentran, aunque sea territorial, sectorial o temporalmente, en una especial situación de subordinación, indefensión o desprotección que les impide el ejercicio de sus derechos como personas consumidoras en condiciones de igualdad».

[157] Christiane Wendehorst, *Safety and Liability Related Aspects of Software*, p. 84.

sal o del fallo o defecto del sistema de IA, ni tan siquiera la presunción de culpa del operador a la que se refiere el considerando núm. 20 de la memoria explicativa que la acompaña [158]. Sin embargo, el Informe del *Expert Group on Liability and New Technologies* (NTF), acerca de un régimen de responsabilidad especial para la IA, aunque parte de la regla general consistente en que la víctima debe probar la causa del daño, admite que la complejidad de la tecnología que interviene puede derivar en una asimetría informativa entre el operador responsable y la víctima que conlleve la imposibilidad de probar el nexo causal o que la prueba resulte excesivamente onerosa para aquélla. Por ello, enumera, en la recomendación núm. 26, una serie de circunstancias que justificarían que el legislador europeo o, incluso, el nacional, incluyeran una *regla general de inversión de la prueba del nexo causal*. Estas circunstancias serían las siguientes: la probabilidad de que la tecnología haya contribuido a ocasionar el daño, la probabilidad de que el daño se hubiera ocasionado o por la intervención de la tecnología o por otra causa que se encuentre dentro de la misma esfera de control, el riesgo de que exista un defecto conocido en la tecnología, aunque su impacto en el nexo causal no sea evidente, el grado de trazabilidad ex post y de inteligibilidad de los procesos gobernados por IA que pueden haber contribuido a causar el daño (asimetría informativa), el grado de acceso posterior y comprensión de los datos recogidos y generados por la tecnología y el tipo y nivel de daño potencial y actual ocasionado [159].

Adicionalmente, se sugiere, en su recomendación núm. 24, *presumir la causalidad* —además de la culpa y de la propia existencia del defecto— siempre que se detecte el incumplimiento de normas de seguridad, cuya observancia hubiera evitado el daño: «Where de damage is of a kind that safety rules were meant to avoid, failure to comply with such safety rules, including rules on

[158] «Precisa que todas las actividades, dispositivos o procesos gobernados por sistemas de IA que ocasionen un daño o perjuicio, pero no estén incluidos en el anexo del Reglamento propuesto deben seguir estando sujetos a la responsabilidad subjetiva; cree, no obstante, que la persona afectada debe poder acogerse a una presunción de culpa del operador, quien debe poder quedar eximido de culpa demostrando que ha observado el deber de diligencia».

[159] Carlos Gómez Ligüerre / Tomás Gabriel García-Micó, «Liability for Artificial Intelligence and other emerging technologies», *InDret*, 1.2020.

cybersecurity, should lead to a reversal of the burden of proving: a) causation, and/or, b) fault, and/or, c) the existence of a defect».

No parece que sea voluntad del legislador europeo, a tenor de la Propuesta de reglamento 2020, la de incorporar alguna de estas recomendaciones para aliviar la carga de la prueba a la víctima, en el texto articulado. Por lo que se deja a la voluntad de los estados miembros, en los ajustes que hagan en sus respectivos ordenamientos jurídicos, el acogerse a todas, algunas o ninguna de ellas.

Estos mecanismos se sumarían, según el *Expert Group on Liability and New Technologies* (NTF), a la presunción *iuris tantum* según la cual la causalidad existe siempre que no sea posible identificar a las personas que manipularon el dispositivo [160].

4.2. *Derecho de acceso a datos personales y no personales*

Lo indicado anteriormente viene acompañado de la obligación de que las tecnologías lleven un sistema de registro del comportamiento de la misma («*logging by design*») [161], información que podría facilitar la prueba a la víctima. Se trata del registro de información relevante acerca de la operación tanto sobre los riesgos de la misma como sobre las implicaciones adversas que pueda tener en los derechos y bienes de terceros. A esta información (datos) debe tener acceso la víctima [162] de suerte que si no lo tiene o el sistema no va equipado convenientemente con ese registro se presumirá *iuris tantum* —sigue recomendando el informe— que se han dado los presupuestos para que nazca la responsabilidad civil a cargo del operador del sistema. El acceso a la «black box» quizá, desde el punto de vista procesal, sirva para fijar indicios [163] que

[160] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 49-53.

[161] Expert Group on Liability and New Technologies (NTF), «Liability for AI and other emerging digital technologies», pp. 47-48.

[162] La consulta de este registro por parte de los sujetos implicados en el evento dañoso no deja de plantear problemas respecto de la protección de datos de carácter personal de terceras personas que en ese registro aparezcan (Ujjayini Bose, «The Black Box Solution», pp. 1325 ss).

[163] Martin Ebers, «Ausservertragliche Haftung für Künstliche Intelligenz – Grundfragen«, Rechtsbrücke núm. 16, Istanbul 2019, p. 45; Gerhard Wagner, «Produkthaftung für Autonome Systeme», *AcP*, 2018, pp. 746-748; Herbert Zech, «Liability for autonomous systems: tackling

permitan establecer presunciones de hecho suficientes para establecer, por ejemplo, el nexo causal. Así se contempla en los *ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights* [164], en cuyo, Principio núm. 20 (1) (c) se contempla el derecho de acceso y de portabilidad de los «datos co-generados» [165], como suele ser el caso en el IoT y en la industria 4.0, cuando sea necesario para establecer hechos, como sería en el supuesto de litigación. Asimismo, el Principio núm.12 (2) (e) establece la posibilidad de conservar los datos por parte del encargado del tratamiento a causa de un proceso judicial que está en marcha o que es muy probable que se inicie o bien porque existe una obligación legal de conservación de los datos [166]. La recién publicada Propuesta de Ley de datos (*Data Act*) [167] establece, en el art. 4, el derecho del usuario de acceder a los datos que el producto o servicio digital contratado genere. La única prohibición respecto del uso de esos datos que establece es la emplearlos para fabricar un producto u ofrecer un servicio que compita en el mercado con el que ha originado los datos. Por tanto, el acceso a los datos

---

specific risks for modern IT», en Sebastian Lohsse / Reiner Schulze / Dirk Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Nomos Verlag, Baden-Baden, 2018, pp. 192-193.

164 Neil Cohen / Christiane Wendehorst, *ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights,* ELI Final Council Draft, p. 146. Online: <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf>. Fecha de la consulta: mayo 2022.

El derecho de acceso (art. 15) y el derecho a la portabilidad de los datos (art. 20) son derechos reconocidos al titular de los datos personales en el RGPD y en los que, a buen seguro, se han inspirado, entre otras fuentes, los Principios mencionados.

165 Los datos co-generados aparecen definidos en el Principio 3 (1) (h): «data to the generation of which a persona other than the controller has contributed, such as by being the subject of the information or the owner or operator of that subject, by pursuing a data-generating activity or owning or operating a data-generating device, or by producing or developing a data-generating product or service» (Neil Cohen / Christiane Wendehorst, *ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights,* ELI Final Council Draft, p. 27).

166 Neil Cohen / Christiane Wendehorst, *ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights,* ELI Final Council Draft, p. 96.

167 Proposal for a regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), Bruselas, 23.2.2022 COM(2022) 68 final.

a los efectos de una posible futura litigación por los daños ocasionados podrá verse amparado legalmente cuando entre en vigor la Data Act.

El acceso a los datos generados por el sistema de IA por parte de los perjudicados puede, como decía, facilitar la carga de probar el comportamiento dañoso y la causalidad. Así, a título de ejemplo, en el Derecho alemán se modificó, en 2017, la *Strassenverkehrgesetz* – StVG para incluir el derecho de la víctima a acceder a esta «caja negra» [§ 63a (3) StVG[168]]. Esta norma fue modificada el 12 de julio de 2021 para introducir los vehículos con funciones autónomas (§ 1g StVG)[169].

Por su parte, en el régimen de responsabilidad especial previsto en la Propuesta de reglamento 2020, para los sistemas de alto riesgo, también se permite el acceso a los datos generados por el sistema de IA, tanto a la víctima como al operador responsable, siempre que se haga de conformidad con la legislación general en materia de protección de datos, sean datos personales o de otro tipo, especialmente, los de carácter técnico (art. 10.2), para los cuales la protección por secreto comercial es clave. En el caso de los primeros deberán ser objeto de anonimización, pseudoanonimización, cifrado, desagregación, aleatorización o cualquier otra medida de seguridad a fin de preservar la privacidad de las personas intervinientes (arts. 32 ss RGPD[170]).

La víctima tiene derecho a que se la informe, cuando los datos son empleados en la adopción de decisiones automatizadas, incluida la elaboración de perfiles, que pudieran conducir a una discriminación, sobre la lógica aplicada, así como la importancia y las consecuencias previstas del tratamiento de los datos personales para el interesado (art. 14 RGPD). El art. 15 RGPD establece el derecho a acceder a los datos personales y a obtener información sobre el tratamiento de ellos. Este derecho a la explicabilidad se da antes de que el sistema de IA adopte una decisión o haga un perfilado. Pero una vez

[168] BGBl I 2017, 1648, 8: Gesetz zur Änderung des Strassenverkehrgesetzes.

[169] <https://www.gesetze-im-internet.de/stvg/BJNR004370909.html>. Fecha de la consulta: mayo 2022.

[170] En el mismo sentido, *vid.* el principio núm. 25 (2) en Neil Cohen / Christiane Wendehorst, *ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights,* ELI Final Council Draft, p. 174.

adoptada la decisión que ocasiona daños a la persona, ¿tiene ésta la posibilidad de que se le explique qué ha pasado y acceder a los datos de la caja negra? El art. 22.3 RGPD permitiría pensar que sí tiene ese derecho cuando establece que el interesado tiene derecho a expresar su punto de vista y a impugnar la decisión que el sistema adoptó. Sin embargo, el RGPD no recoge de forma explícita el derecho a la explicabilidad en estos casos [171]. En cualquier caso, este derecho debería ser compatible con la protección del sistema de IA por derechos de propiedad intelectual y de secreto comercial [172].

El acceso a estos datos, que son datos no divulgados, permite que se investiguen las causas de que un sistema de IA haya funcionado mal causando daños. En estos casos, el acceso a los datos de entrenamiento del sistema de IA deviene relevante. Esta es una cuestión, en opinión de López-Tarruella [173], de orden público en el sentido de que el interés por conocer donde ha fallado el sistema de IA para solucionar el problema y que no vuelva a suceder en el futuro no solo interesa a la víctima y al operador del sistema de IA, como propone la propuesta de reglamento 2020, sino que interesa a un más amplio espectro de personas y entidades, como son asociaciones de consumidores, centros de investigación, autoridades públicas, aseguradoras. Facilitar la investigación de los errores cometidos por el sistema de IA contribuye a que se haga realidad una IA esté centrada en el ser humano [174], donde la explicabilidad y la transparencia ocupan un lugar destacado. Debería pues hacerse compatible el derecho de acceso a los datos con la normativa sobre secreto comercial o sobre

[171] Sandra Wachter / Bernt Mittelstadt / Luciano Floridi, «Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation», *International Data Privacy Law*, vol. 7, n. 2, 2017. Online: <https://ssrn.com/abstract=2903469>. Fecha de la consulta: mayo 2022.

[172] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del reglamento 2016/679, p. 19. Online: <https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf>. Fecha de la consulta: mayo 2022.

[173] Aurelio López-Tarruella Martínez, *Propiedad intelectual e innovación basada en datos*, Dykinson, Madrid, 2021, p. 195.

[174] AI HLEG, «Directrices éticas para una IA fiable», 8 de abril de 2019, <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Fecha de la consulta: mayo 2022.

propiedad intelectual. De hecho, en la Resolución sobre derechos de propiedad intelectual para el desarrollo de tecnologías relativas a la inteligencia artificial de 20 de octubre de 2020[175], el Parlamento europeo pide a la Comisión que tenga en cuenta y aplique adecuadamente en toda la legislación relativa a la IA los siete requisitos esenciales indicados en las directrices del AI HLEG.

Por su parte, la AIA no establece explícitamente un derecho de acceso a los datos ni siquiera un derecho a la explicabilidad por el mal funcionamiento del sistema de IA. Establece normas destinadas a prevenir que aparezcan sesgos mediante la adopción de un sistema de gestión de riesgos (art. 9 AIA) y de calidad (art. 17 AIA), facilitar la detección de los sesgos mediante la elaboración de documentación técnica (art. 11 AIA), registro de las operaciones (art. 12 AIA) y supervisión humana (art. 14 AIA), además de que se debe informar adecuadamente a los usuarios de estos sistemas (art. 13 AIA). En relación directa con los datos, el art. 10 AIA, en la versión adoptada en el texto de compromiso hecho público el 13 de enero de 2022, admite que un sistema de IA libre absolutamente de errores es imposible, por lo que se trata de adoptar las medidas que minimicen en la medida de lo posible la existencia de errores y, sobre todo, de sesgos[176]. El art. 10 AIA establece que los sistemas de IA de alto riesgo que se desarrollen con conjuntos de datos deben responder a unas prácticas apropiadas de gobernanza y administración en relación con la elección, recopilación, etiquetado y otras técnicas de preparación. Los conjuntos de datos deben estar libres de errores, ser completos y representativos, por tanto, libres de sesgos. Sin embargo, el derecho de acceso a estos conjuntos de datos está ausente. Incluso el art. 3 AIA cuando alude a la obligación de los proveedores de sistemas de IA de alto riesgo de colaborar con las autoridades competentes solo se refiere al acceso a los registros de operaciones ejecutadas

[175] Resolución del Parlamento europeo «Derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial», núm. 4, de 20 de octubre de 2020, 2020/2015(INI). Online: <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_ES.pdf>. Fecha de la consulta: mayo 2022.

[176] «The modification in Article 10(3) is meant to acknowledge the fact that training, validation and testing data sets can never be completely free of errors and to clarify that the requirement is to ensure that they are free of errors to the best extent possible» [Interinstitutional File: 2021/0106(COD)].

automáticamente por el sistema manteniendo la confidencialidad de la información que obtengan (art. 70 AIA). No se hace mención de la posibilidad de que las autoridades puedan acceder a datos de entrenamiento.

Tampoco impone la AIA una obligación de conservación de los conjuntos de datos como, en cambio, el *Libro Blanco en IA* sí establecía [177].

En definitiva, como advierte López-Tarruella, «en la actualidad, cuando un sistema de IA llega a decisiones o predicciones presuntamente erróneas o discriminatorias, no existe ninguna disposición en el acervo comunitario que establezca claramente la obligación de los titulares de dichos sistemas de ofrecer acceso a los datos de entrenamiento para investigar las causas de esos errores o sesgos» [178].

Finalmente, para facilitar el acceso a los datos sería recomendable que se desarrollaran APIs (*application programme interfaces*) estándar que permitieran el acceso a los datos a las personas autorizadas independientemente el lugar donde estuvieran almacenados los datos, pues una de las características, de éstos es la deslocalización. Además, ello permitiría la portabilidad de esos datos [179].

III. Ajustes legales futuros en el derecho de la responsabilidad civil en materia de inteligencia artificial

Como he advertido al inicio de este trabajo, las instancias europeas consideran que la introducción de un régimen de responsabilidad especial por los daños que ocasione una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA no requiere una reforma de calado de la responsabilidad civil en los derechos nacionales, sino tan solo unos ajustes mínimos. Por su parte, la estrategia nacional española sobre inteligencia artificial no contiene ninguna alusión de relieve al tema que me ocupa [180].

[177] *Libro blanco en IA*, p. 24.

[178] Aurelio López-Tarruella Martínez, *Propiedad intelectual*, p. 190.

[179] European Data Protection Supervisor, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – An European approach to excellence and trust*, 29 de junio de 2020.

[180] <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf>. Fecha de la consulta: mayo 2022.

En el caso del ordenamiento jurídico-privado español debe tenerse en cuenta que todavía no se ejecutado la reforma en profundidad que las normas sobre responsabilidad del CC requieren. Por eso, voy a partir de dos escenarios a la hora de abordar la cuestión que rubrica estas líneas: el primero parte de la situación de *lege lata* sin esperar a que la Propuesta de reglamento se convierta en norma aplicable; mientras que el segundo se centra en la situación de *lege ferenda*, para la cual tomaré como base la Propuesta de reforma del CC de la APDC [181]. Vayamos a cada uno de ellos.

a. En relación con las normas vigentes de responsabilidad civil se podría, por un lado, modificar el tenor de algunas normas como, por ejemplo, las de los arts. 1903, 1905 e, incluso, el 1908 CC con la finalidad de introducir los daños ocasionados por sistemas de IA, lo que se puede hacer de tres maneras: primera, adicionando, donde fuera menester, la expresión «sistema de IA»; segunda, añadiendo un apartado en cada uno de los preceptos en los que se indicara que lo establecido en el apartado anterior también se aplica a los sistemas de IA y, la tercera, insertando un nuevo apartado donde se describiera el supuesto de hecho relacionado con el sistema de IA, lo que, en su caso, permitiría destacar algún elemento particular del mismo y diferente de los supuestos de hecho regulados en los apartados del mismo precepto. Reconozco que la intervención legislativa mínima es más fácil de hacer en los arts. 1905 y 1908 CC que en el art. 1903.4 CC. En este último caso, requiere plantearse cuestiones que generan un efecto disruptivo legal más relevante en la medida en que lleva a cuestionarse un principio fundamental en el que se asienta el Derecho, cual es el antropocentrismo. Y, además, supone plantearse la aplicación (o no) de la acción de regreso prevista en el art. 1904 CC del empresario (principal) respecto de su auxiliar (sistema de IA), el cual debería de gozar entonces de su propio peculio.

Por otro lado, deberían hacerse intervenciones en leyes especiales tales como la citada legislación sobre responsabilidad civil por circulación de vehí-

[181] Asociación de Profesores de Derecho civil, *Propuesta de Código civil. Libros quinto y sexto*, Tirant Lo Blanch, Valencia, 2016, pp. 319 ss.

culos a motor para restar protagonismo al «conductor» y dárselo quizá al «propietario» del vehículo, añadir la importancia de acceder a los datos que genere el sistema de IA para la víctima, entre otras cuestiones [182]. Otra norma en la que se debería intervenir sería en el TRLGDCU en la que contemplando específicamente al «consumidor» como persona afectada por los daños que ocasiona el sistema de IA, se introduzca un régimen especial de carácter objetivo junto a los ya existentes, lo que podría hacerse en un solo precepto. Incluso modificar el tenor de alguno de los regímenes existentes como, por ejemplo, el que tiene que ver con la responsabilidad por la prestación de servicios para incluir los que se prestan empleando sistemas de IA y, por supuesto, la responsabilidad del fabricante, de la que me ocupo en la segunda parte de este trabajo. Alguna previsión específica debería establecerse en materia de consumo, por ejemplo, en relación con los drones de recreo u ocio que quedan excluidos de las normas específicas que los regulan [183].

Finalmente, los ajustes también deberían alcanzar, por un lado, a la Ley orgánica reguladora del derecho al honor, intimidad personal y familiar y propia imagen [184] en lo que respecto a la intromisión ilegítima en estos derechos fundamentales empleando sistemas de IA de, por ejemplo, reconocimiento facial, reconocimiento de voz, comentarios falsos en redes sociales que afectan a la reputación de la persona, sistemas de rating, etc. Por otro lado, la Ley orgánica de igualdad efectiva de mujeres y hombres [185] también debe sufrir algunas modificaciones en la medida en que parte de la base de que el comportamiento discriminatorio proviene de una persona mientras que, en la actualidad, éste proviene de un sistema de IA cuyas decisiones no siempre son explicables ni existe explícitamente un derecho de acceso a los

[182] Es, en definitiva, lo que suele hacer Alemania. A saber, modifica su derecho interno sin esperar a que las proyectadas regulaciones europeas se conviertan en normas vigentes y aplicables marcado de esta guisa, en varias ocasiones, el camino tanto a las instancias europeas como a los derechos nacionales. *Vid.,* al respecto, Arantzazu Vicandi Martínez, «El contrato de seguro de automóvil frente a los coches autónomos: luces y sombras de los Smart cars», *REDS*, enero-junio 2019, núm. 14, pp. 101 ss.

[183] Susana Navas Navarro, «Smart robots», pp. 82-109.

[184] Ley orgánica 1/1982, de 5 de mayo, BOE núm. 115, de 14 de mayo.

[185] Ley orgánica 3/2007, de 22 de marzo, BOE núm. 71, de 23 de marzo.

datos empleados por aquél, salvo el limitado derecho de acceso admitido en caso de datos personales.

b Centrándome ahora en la Propuesta de modificación del CC en materia de responsabilidad por parte de la APDC, la solución más factible sería añadir un Capítulo IX que llevara por título *De los daños causados por el uso de sistemas de inteligencia artificial*. Otra opción sería introducir en el Capítulo VI «De la responsabilidad civil empresarial» una nueva sección, la sección 3.ª, que llevara por título *De la responsabilidad derivada del uso de sistemas de inteligencia artificial* o, incluso que las normas relativas a esta responsabilidad se antepusieran a las de la responsabilidad derivada de productos o servicios defectuosos que, en la actualidad, figura como sección 2.ª pasando a ser la 3.ª En esta dirección, en primer lugar, aparecerían las normas especiales en materia de responsabilidad civil general por el uso de sistemas de IA seguidas, en segundo lugar, de las normas especiales del régimen especial de responsabilidad del fabricante que también deberían ser objeto de adaptación a una futura revisión de la regulación comunitaria. Ahora bien, teniendo en cuenta que un particular puede usar un sistema de IA que puede ocasionar daños y que las instancias europeas consideran que el «operador», que es el sujeto responsable, puede ser un particular o una empresa quizá la primera alternativa, esto es, añadir un nuevo Capítulo sería la solución más adecuada.

De otra parte, la regla de la responsabilidad proporcional en materia de causalidad en relación con los problemas de incertidumbre que se generan en un entorno operado por sistemas de IA con o sin interacción con humanos debe tenerse en cuenta a la hora de plantearse una posible regulación de la responsabilidad civil por los daños ocasionados [186].

Finalmente, incluir este régimen especial de responsabilidad en el CC implicaría asimismo modificar la Propuesta de CC en materia de prescrip-

[186] En la misma línea, *vid.* Miquel Martín Casals, «Causation and Scope of Liability», p. 227. Del mismo autor, *vid.* «Proportional Liability in Spain», en Miquel Martín Casals / Diego M. Papayannis, *Uncertain Causation in Tort Law*, Cambridge, Cambridge University Press, 2016, pp. 43-66.

ción en la medida en que los plazos de las pretensiones, así como el inicio del cómputo, no coincide con el previsto en el Libro VI.

Sea lo que fuere, lo más seguro sea que el legislador español, en lugar de aprovechar la oportunidad para acometer la deseada reforma del CC, en esta y otras materias, se limite a regular aquellos aspectos, que el futuro Reglamento deje para su concreción a los estados miembros o que sencillamente no contemple, en una ley especial, en la que «replique», además, las normas de aquél. Previsiblemente, lo haga mediante un decreto-ley y no mediante el procedimiento legislativo correspondiente. Hay que tener en cuenta que el ámbito de aplicación subjetivo de la Propuesta de reglamento 2020 incluye tanto a personas físicas como jurídicas que pueden ser víctimas de los daños ocasionados al operar sistemas de IA (art. 1). Por ello, no me parece que el TRLGDCU sea la sede adecuada para incluir esta nueva regulación. De otra parte, si el instrumento legislativo empleado para regular esta materia fuera una Directiva y no un Reglamento como se pretende, quizá, se daría una mayor flexibilidad para que los estados miembros pudieran modificar sus respectivos regímenes de responsabilidad allá donde fuere necesario. De todos modos, en el caso del legislador español, a la vista de las últimas incorporaciones de Directivas al derecho español, tampoco resulta probable que se acometiera la tan esperada reforma del CCE, por el hecho de que el régimen de responsabilidad se regule en una Directiva y no en un Reglamento.