

Responsabilidad civil e Inteligencia artificial*

SUSANA NAVAS NAVARRO

Catedrática de Derecho civil. Universidad Autónoma de Barcelona.

I. INTRODUCCIÓN

Desde la resolución del Parlamento europeo de 16 de febrero de 2017 acerca de unas reglas en materia de derecho civil sobre robótica¹, la preocupación tanto de las instituciones europeas como de la academia acerca de qué ajustes normativos deben diseñarse para resarcir a la víctima de daños causados por un sistema de inteligencia artificial (IA) no ha hecho más que aumentar. En efecto, a la referida resolución le suceden múltiples documentos y materiales de trabajo de los cuales me parece importante destacar los siguientes: el Informe del Grupo de expertos en responsabilidad y nuevas tecnologías (NTF), “Responsabilidad por inteligencia artificial y otras tecnologías emergentes”, de 28 de noviembre de 2019², el Libro blanco “Sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza”³ y, finalmente, la Resolución del Parlamento europeo de 20 de octubre de 2020 con recomendaciones para una “Propuesta de Reglamento en materia de responsabilidad civil por el uso de inteligencia artificial”⁴. A ellos deben añadirse los trabajos que se están pergeñando sobre una más que necesaria reforma de la *Directiva 85/374/CEE de 5 de julio de 1985 sobre la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por productos defectuosos*⁵,

como, por ejemplo, los que está llevando a cabo, entre otros, el European Law Institute (ELI)⁶.

Abordar el tema de la responsabilidad civil por los daños ocasionados por sistemas de IA implica enfrentarse, en esencia, a tres aspectos diferenciados desde un punto de vista teórico, pero que acaban confluyendo en la práctica. El primer aspecto se centra en los presupuestos generales para que nazca la responsabilidad civil, el segundo en el régimen específico de responsabilidad civil cuando los daños son ocasionados por sistemas de alto y bajo riesgo y, el tercero, en la responsabilidad civil del fabricante de un sistema de IA que pueda considerarse defectuoso. De los tres me he ocupado recientemente, si bien, en esta contribución en el número 100 de *El Cronista: El estado social y democrático de Derecho*, dirigida por el admirado Prof. Santiago Muñoz Machado, me centraré en el segundo y tercer aspecto.

II. DAÑOS OCASIONADOS POR SISTEMAS DE ALTO Y BAJO RIESGO. DUALIDAD DE RÉGIMENES DE RESPONSABILIDAD

1. Sistemas de inteligencia artificial de “alto” y “bajo” riesgo. Su relación con la Propuesta de reglamento de inteligencia artificial

Los textos europeos citados en relación con la responsabilidad civil por el uso de sistemas de IA distinguen entre tecnología de “alto riesgo”⁷ (por ejemplo, automóviles sin conductor, drones, un brazo quirúrgico robotizado⁸) y la tecnología de “bajo riesgo” (por ejemplo, una aspiradora como Roomba, un chatbot como Alexa, algunas de las herramientas LegalTech).

* Las reflexiones que siguen toman como base mi monografía “Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación”, Comares, Granada, 2022.

Estando en imprenta este trabajo se publicaron la Propuesta de Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual en relación con la inteligencia artificial [COM(2022) 496 final] y la Propuesta de Directiva revisando la responsabilidad por defectos en los productos [COM(2022) 495 final]. Por eso no han podido ser tenidas en cuenta en este trabajo. En próximas publicaciones serán analizadas con detenimiento.

¹ P8_TA(2017)0051.

² <LiabilityforAlandotheremergingtechnologies.pdf>. Fecha de la consulta: septiembre 2022.

³ COM(2020) 65 final, 19.2.2020.

⁴ <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html>. Fecha de la consulta: septiembre 2022.

⁵ DOUE L 210, 7.08.1985. Será abreviada como “Directiva 85/374/CEE”.

⁶ C. TWIGG-FLESNER, “Guiding Principles for Adapting the Products Liability Directive for the Digital Age”, *ELI Innovation Paper Series*, p. 5. Online: <europeanlawinstitute.eu>. Fecha de la consulta: septiembre 2022.

⁷ Libro Blanco en IA, pp. 16-17.

⁸ S. NAVAS NAVARRO (dir.), *Salud e Inteligencia artificial desde el Derecho privado*, Comares, Granada, 2021.

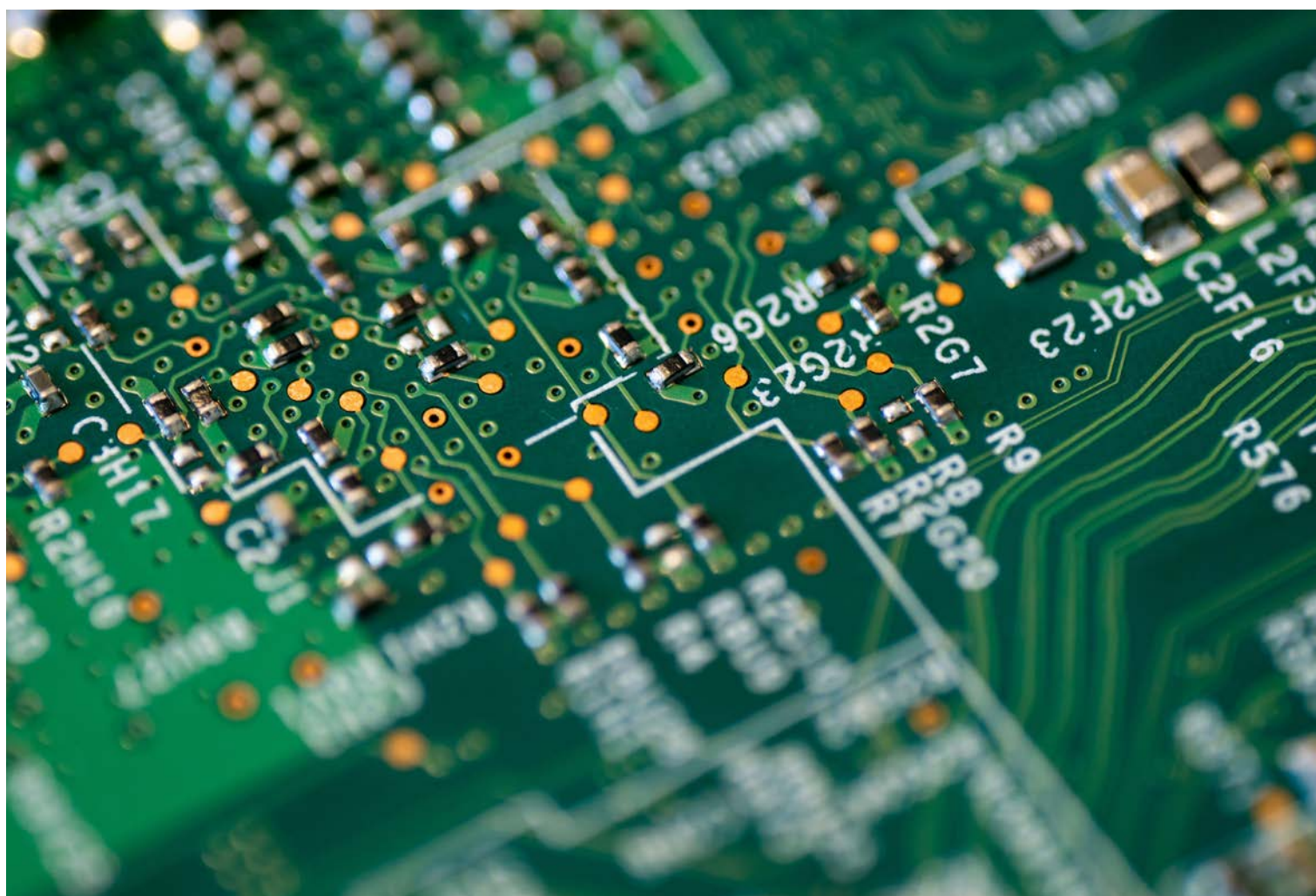


Foto de Magnus Engø en Unsplash.

En las recomendaciones para una Propuesta de reglamento 2020, en consonancia con el *Libro Blanco en IA*, se define tan solo 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)⁹. Es lo que se conoce como “daño significativo”.

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 dada de sistema de IA de alto riesgo parece pensar en aquel sistema cuyo uso o manejo ocasiona daños en

espacios abiertos al público o 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 o de un dron) sino también que se produzcan “daños colectivos” que pueden afectar a la sociedad o a la economía en general (v. gr., manipulación del comportamiento 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). Sin embargo, dentro de la categoría de sistema de alto riesgo entran aquellos sistemas que, aunque no produzcan daños a una pluralidad de personas no identificadas cuando se pone en funcionamiento el sistema, ocasionan daños, en espacios cerrados, a una persona concreta que tampoco se conoce con carácter previo al inicio del funcionamiento de aquél como sería el caso de un sistema de IA que diagnostica un determinado tipo de cáncer y propone un tratamiento específico.

En un anexo al futuro Reglamento se pretenden enumerar los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan (art. 4.2). De hecho, el *Libro Blanco en IA* hacía referencia a los sectores que consideraba críticos como el transporte o la asistencia¹⁰, dentro de la cual, se podría comprender a la sanidad.

⁹ G. WAGNER, “Haftung für Künstliche Intelligenz – Eine Gesetzinitiative des Europäischen Parlaments”, *ZEuP*, 2021, p. 554.

¹⁰ *Libro Blanco en IA*, pp. 16-17.

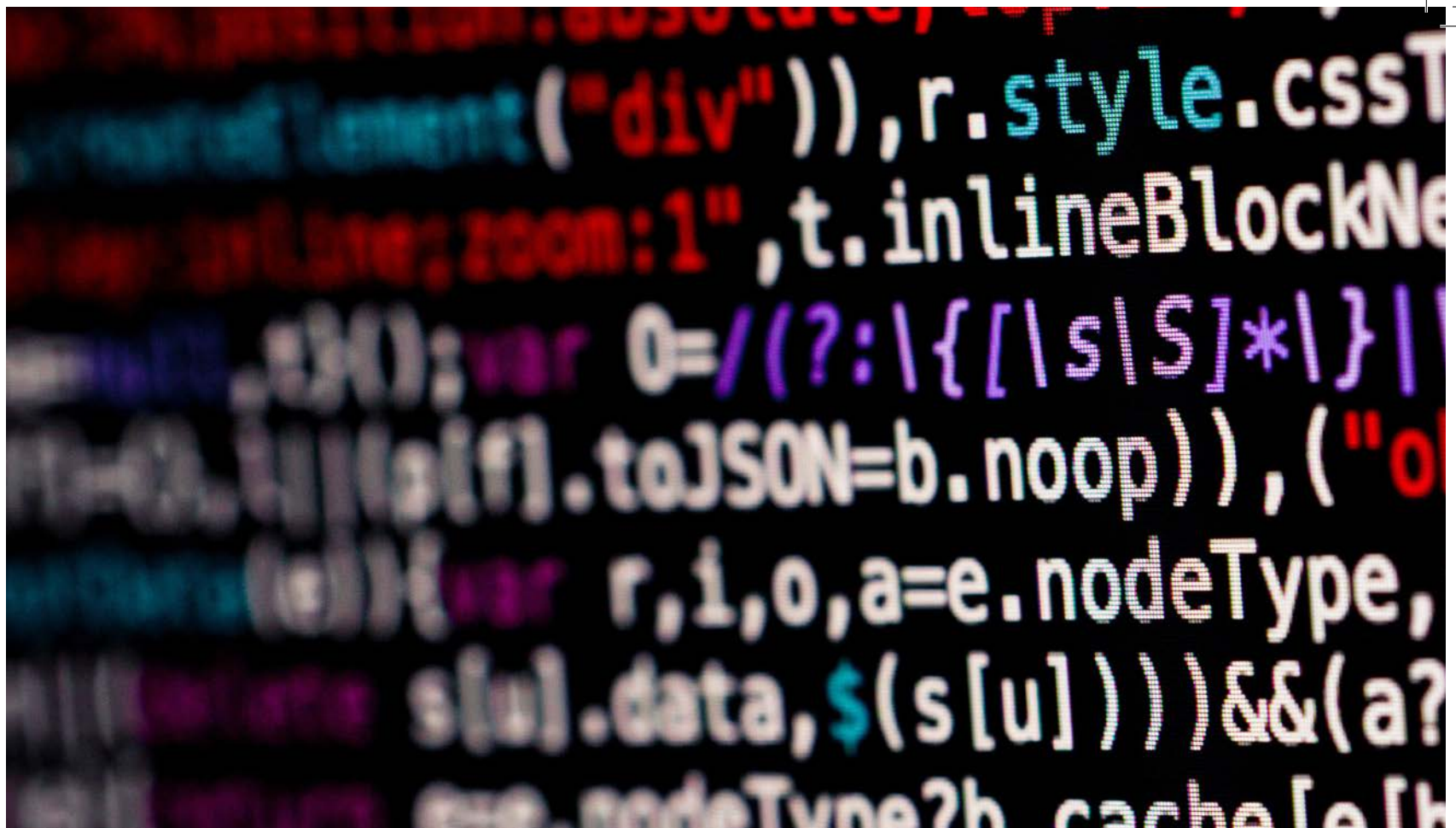


Foto de Markus Spiske en Unsplash.

En este aspecto convendría tener en cuenta, cuando se elabora ese listado, los sectores o materias referidos en el Anexo III de la AIA¹¹, 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 establecerá 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 exigidos por la AIA para proceder a su comercialización, puesta en servicio o utilización (Capítulo 2 del Título III, arts. 8 y 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 de reglamento recomendada por el parlamento europeo para los sis-

temas 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.

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 individuos¹², los *sistemas de alto riesgo* que deben cumplir unos requisitos obligatorios *ex ante* y *ex post* comercialización o puesta en servicio (arts. 8 y 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, que los contemplen, elaborados por ellos o por las organizaciones a las que pertenecen (art. 69 AIA).

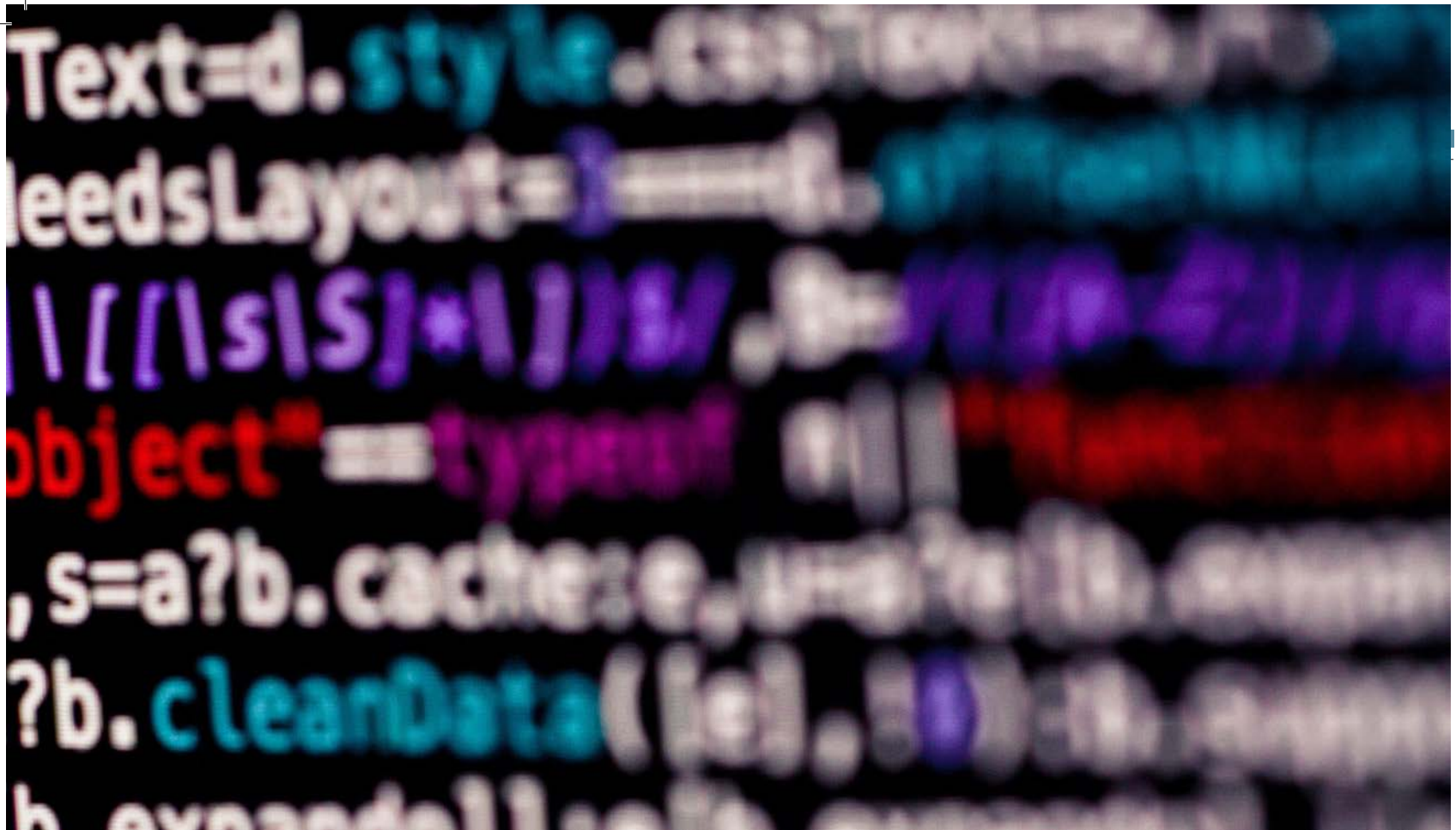
2. Regímenes de responsabilidad para el operador del sistema de inteligencia artificial

En las recomendaciones para una Propuesta de reglamento 2020 se sugiere, para los sistemas de alto riesgo, un régimen de responsabilidad civil basado precisamente en el riesgo para

¹¹ Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, COM(2021) 206 final. La propuesta se puede consultar en: <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF>. Fecha de la consulta: septiembre 2022. A lo largo de este trabajo será abreviada como AIA en referencia a como se la conocerá "Artificial Intelligence Act".

Los ámbitos listados en el Anexo III de la AIA 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.

¹² Consistentes 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).



las personas y las cosas que una actividad física o virtual, un dispositivo o un proceso gobernado por un sistema de IA pueda conllevar. Es decir, lo que conocemos como responsabilidad objetiva.

Este nuevo marco regulatorio parte de la “gestión del riesgo”¹³. 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 en un mismo sujeto.

Las recomendaciones del Parlamento europeo para una Propuesta de reglamento en materia de responsabilidad civil, siguiendo el Informe del *Grupo de expertos en inteligencia artificial y tecnologías emergentes*, establece que pueden ser dos o más los “operadores” del sistema de IA¹⁴. En particular:

- a) la persona que principalmente decide y se beneficia del uso de la tecnología (*frontend operator* u *operador inicial*, art. 3 letra e de la futura Propuesta de reglamento), 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*¹⁵, art. 3 letra f futura Propuesta de reglamento) 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, se propone en las recomendaciones para una futura Propuesta de reglamento como definición de “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. La responsabilidad solidaria es vista como la mejor solución (art. 11), sin perjuicio de las acciones de regreso del que satisfizo la indemnización a la persona afectada frente a los otros corresponsables (art. 12).

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). Este régimen está presente en todos los ordenamientos

¹³ EU Parliament Resolution on 16 February 2017 and “Building a European Data Economy”, 10.1.2017 COM(2017), 9 final.

¹⁴ G. WAGNER, “Haftung für Künstliche Intelligenz”, p. 553; M.^a L. ATIENZA NAVARRO, *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022, pp. 292-297.

¹⁵ P. 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).

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 objetivada¹⁶.

III. RESPONSABILIDAD DEL FABRICANTE DE UN SISTEMA DE INTELIGENCIA ARTIFICIAL

La Directiva 85/374/CEE se encuentra en revisión con la intención de ofrecer acomodo en su seno, con las modificaciones pertinentes, a los sistemas de IA y demás tecnología emergente¹⁷. Es ya evidente que los productos que se comercializan en el mercado interior han ganado en complejidad al comprender

¹⁶ P. ÁLVAREZ OLALLA, "Propuesta de reglamento", pp. 9-10; M.^a L. ATIENZA NAVARRO, *Daños causados por inteligencia artificial*, pp. 310-313.

¹⁷ European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics*, COM(2020) 64 final.

elementos digitales que van cambiando, actualizándose, mejorándose, que se confunden en ocasiones con los servicios, también prestados digitalmente; productos que se comunican e interactúan con otros productos y servicios mediante diferentes sistemas, que generan un importante flujo de datos, los cuales constituyen un bien en sí mismos, que emplean sistemas de IA autónomos para tomar decisiones tras el procesado veloz de cantidades ingentes de datos. Estas nuevas realidades hacen que se tengan que clarificar determinados conceptos que, en la norma comunitaria, corresponden a un mundo analógico y no digital. Y, si bien es cierto que, en 1988, la Comisión europea confirmó que el *software* podía considerarse un producto en el sentido de la Directiva 85/374/CEE¹⁸, en realidad, se estaba refiriendo al *software* estándar predeterminado producido en masa (*locked software*) que, una vez instalado, no cambia, no se actualiza ni mejora.

A pesar de la revisión de conceptos tales como el de producto, el de defecto, el momento de puesta en circulación, de productor, de los daños resarcibles y la carga de la prueba para la víctima, parece que el sentir de las instancias europeas está en la línea de entender que la Directiva 85/374/CEE sigue siendo una herramienta útil a la que una serie de ajustes menores permitirá adaptarse fácilmente a la nueva realidad del mercado¹⁹. En esa revisión deben especialmente tenerse en cuenta otras normas comunitarias, tales como la *Directiva (UE) 2019/770, del Parlamento europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales*²⁰ y la *Directiva (UE) 2019/771, del Parlamento europeo y del Consejo de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes*²¹. En cualquier caso, el criterio de imputación basado en el riesgo seguirá vigente. Así, la responsabilidad del fabricante seguirá siendo un supuesto más de responsabilidad objetiva. Esto deja entrever las dificultades que podrá haber en la coordinación de esta Directiva con la regulación futura de la responsabilidad civil por el uso de sistemas de IA que he esbozado en el apartado anterior.

1. Concepto de producto

El concepto de producto en la Directiva 85/374/CEE se centra en los bienes tangibles con la excepción de la electricidad (art. 2) excluyendo claramente a los servicios²². Si bien no existe problema en comprender en su ámbito de aplicación aquel bien tangible que incorpora un elemento digital como puede ser un *software*, sí que es cierto que éste es concebido

¹⁸ G. WAGNER, "Robot Liability", p. 44; BEUC, "Products Liability 2.0. How to make EU rules fit for consumers in the digital age", 7 de mayo de 2020, p. 13.

¹⁹ Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre la aplicación de la Directiva del Consejo relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85/374/CEE) [COM(2018) 246 final] [SWD(2018) 157 final]. En la doctrina especialista en Derecho del consumo, vid. G. HOWELLS, "Protecting Consumer Protection Values in the Fourth Industrial Revolution", *J. Consum. Policy* (2020) 43: 145-157, pp. 148-160.

²⁰ DOUE L 136, 22.05.2019. Abreviada como "Directiva 2019/770".

²¹ DOUE L 136/28, 22.5.2019. Abreviada como "Directiva 2019/771".

²² Así, por ejemplo, lo reconoce el TJUE en el caso C-495/10 (*Centre hospitalier universitaire de Besançon*) en sentencia de 21 de diciembre de 2011.

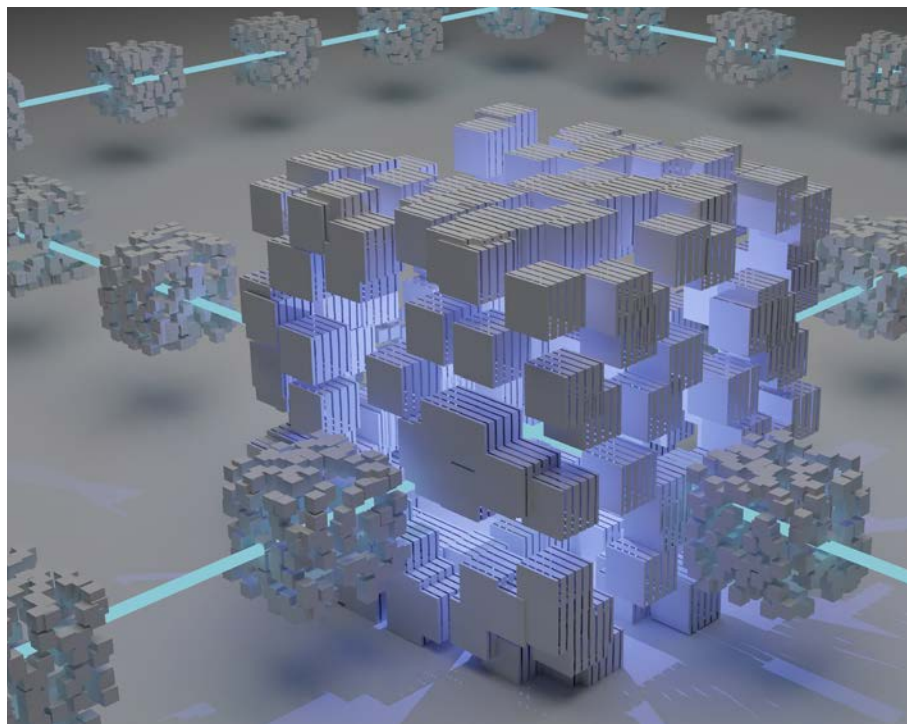


Foto de GuerrillaBuzz Crypto PR en Unsplash.

como un elemento estático, esto es, un elemento digital que es estándar y producido en masa (v. gr., un electrodoméstico inteligente). Más problemático resulta, para poder comprenderlo en el concepto de producto, aquel contenido digital incorporado en el bien tangible que es dinámico, que se actualiza con mucha frecuencia y que puede llegar a ser mucho más importante que el propio bien tangible en el cual aparece integrado o, aunque no aparezca integrado, interactúa con él de tal manera que su ausencia afecta a la operatividad del bien. De ahí que deba ampliarse el concepto de producto para comprender este supuesto acogiendo la definición de “bien con elementos digitales” ya dada por la Directiva 2019/770 (art. 2.3: “todo objeto mueble tangible que incorpore contenidos o servicios digitales o esté interconectado con ellos de tal modo que la ausencia de dichos contenidos o servicios digitales impediría que los bienes realizaran sus funciones”) en aras a la coherencia del marco jurídico en el mercado digital (art. 3.3 ELI Draft²³).

De otra parte, el contenido digital en sí mismo considerado, por ejemplo, el *stand-alone-software* (en nuestro caso, el *stand-alone-AI system*) podría merecer la consideración de “producto”, si bien si está hecho a medida, quizá se trate más bien de un servicio que conlleva un resultado. También cabe considerarlo directamente un servicio digital como es el supuesto del SaaS (*software as a service*) que, en el caso que me ocupa es AlaaS (*artificial intelligence as a service*)²⁴. En este sentido, debería englobarse dentro del concepto de producto también al contenido y servicio digital²⁵ definido de acuerdo con las Directivas 2019/770 (art. 2.1 y 2) y 2019/771 (art. 2.6 y 7): 1) “contenido digital”: los datos producidos y suministrados en formato digital; 2) “servicio digital”: a) un servicio que permite al consumidor crear, tratar, almacenar o consultar datos en formato digital, o b) un servicio que permite compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos.

2. Concepto de defecto

La cuestión que debe plantearse en relación con el concepto de defecto es si la noción dada por la Directiva 85/374/CEE sigue siendo válida para la era digital en la que la pérdida de conectividad o de datos y los ciberataques originan daños que no siempre se corresponden con los tipos de daños previstos por la Directiva 85/374/CEE. Debe tenerse en cuenta que, en los bienes digitales, los defectos se refieren muy probablemente a otras circunstancias más allá de las previstas en el art. 6.1. En este sentido, quizá, manteniendo el concepto de defecto como la falta de seguridad del producto que cabría legítima-

mente esperar (“*consumer expectations test*”) para delimitar la noción abstracta de defecto, se podrían ampliar las circunstancias que la norma tiene en cuenta, incluyendo, por un lado, otras como, por ejemplo, el tipo de usuario concernido, la ciberseguridad y la fortaleza de un sistema de IA, el flujo de datos, la privacidad desde el diseño y por defecto (arts. 25 RGPD), la funcionalidad, interoperatividad y compatibilidad del sistema de IA²⁶, y, por otro lado, revisando la circunstancia relativa al momento de puesta en circulación del producto. En efecto, el hecho de que un producto digital y, en particular, un sistema de IA, no sea estático, sino dinámico al irse actualizando (*updates*) o incluso mejorando (*upgrades*) pone en cuestión, de una parte, el momento de su puesta en circulación y, de otra, la condición de que un producto mejor o mejorado puesto en circulación después no suponga que el anterior sea defectuoso (art. 6.2 Directiva 85/374/CEE)²⁷.

3. Momento de puesta en circulación del sistema de inteligencia artificial

El momento de puesta en circulación del producto es una de las circunstancias que establece el art. 6.1 Directiva 85/374/CEE (art. 137 TRLGDCU) modulando el concepto de defecto. De hecho, el momento de la puesta en circulación ha representado la clave de bóveda del régimen jurídico previsto en la norma comunitaria pues en torno a él pivotan, por ejemplo, las causas de exoneración de la responsabilidad del fabricante (art. 7 Directiva 85/374/CEE, art. 140 TRLGDCU).

En un mercado analógico en el que se fabrican bienes tangibles que, si bien tienen incorporado algún elemento digital, éste es estático, es decir, no sufre ningún cambio, el momento de su puesta en circulación en el mercado es igualmente un momento temporal estático. Ahora bien, en un mercado digital donde el bien que se fabrica puede ser no sólo tangible sino, sobre todo, intangible y, además, éste se halla incorporado al primero de suerte que sin él deja de funcionar o que, incluso se comprenden servicios digitales, el momento de puesta en circulación del sistema de IA o más ampliamente del “producto digital” deja de ser un momento temporal estático. En efecto, los productos digitales van configurándose constantemente a partir de actualizaciones (*updates*) y mejoras (*upgrades*) que hacen difícil determinar cuándo el bien se considera puesto en circulación. ¿Debe considerarse que una actualización del producto forma parte de éste en el momento en que se puso en circulación, aunque sea de forma retroactiva? ¿Deben considerarse momentos de puesta en circulación diferentes, una para el producto, otra para cada actualización y mejora? Incluso el concepto de puesta en circulación podría repensarse. De hecho, se ha propuesto como alternativa el “momento

²³ ELI Draft of a Revised Product Liability Directive, p. 8. Online: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf>. Fecha de la consulta: septiembre 2022. Vid., asimismo, M.^a L. ATIENZA NAVARRO, *Daños causados por inteligencia artificial*, pp. 145-147.

²⁴ T. S. CABRAL, “Liability and Artificial Intelligence in the EU: Assessing the adequacy of the current Products Liability Directive”, MJ, 2020, p. 8; C. WENDEHORST, *Safety and Liability Related Aspects of Software*, EU Commission, 2021, p. 60; ELI Draft of a Revised Product Liability Directive, p. 10.

²⁵ R. H. WEBER / D. N. STAIGER, “New Liability Patterns in the Digital Era”, en Tatiana Eleni Synodinou et al. (ed.), *EU Internet Law – Regulation and Enforcement*, Springer, 2017, p. 203.

²⁶ ELI Draft of a Revised Product Liability Directive, p. 16; M.^a L. ATIENZA NAVARRO, *Daños causados por inteligencia artificial*, pp. 161-163.

²⁷ C. TWIGG-FLESNER, “Guiding Principles”, pp. 7-8; BEUC, “Products Liability 2.0: How to make EU rules fit for consumers in the digital age”, 7 de mayo de 2020, p. 14; ELI Reponse to the public consultation on civil liability, Online: <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_Public_Consultation_on_Civil_Liability.pdf>. Fecha de la consulta: septiembre 2022, p. 16; F. P. PATTI, “Machine Learning and European Contract Law”, en A. JANSSEN / H. 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. 114.

en que se pone a disposición o se introduce un producto o servicio en el mercado” (art. 3.2 del Reglamento (UE) 2019/1020 del Parlamento europeo y del Consejo de 20 de junio de 2019 relativo a la vigilancia del mercado y la conformidad de los productos²⁸.

Las actualizaciones consisten en cambios menores que no necesitan pasar el proceso de conformidad previsto en la norma de que se trate; mientras que, en el supuesto de mejoras, se realizan modificaciones relevantes que requieren cumplir con las condiciones de precomercialización establecidas en las normas hasta alcanzar el certificado de conformidad CE. No deberían, en mi opinión, recibir el mismo tratamiento jurídico las actualizaciones que las mejoras del producto a efectos de determinar el momento de su puesta en circulación.

4. Concepto de productor

Otro concepto que debería revisarse es el del “productor”. Según las normas de responsabilidad civil del fabricante, éste, de acuerdo con el concepto legal de productor establecido (art. 3 Directiva 85/374/EEC, art. 138 TRLGDCU), es el que responde por los daños que ocasione un producto defectuoso frente a terceros. En concreto, se considera fabricante a la persona que fabrica un producto acabado, que produce una materia prima o que fabrica una parte integrante, y toda aquella persona que se presente como productor poniendo su nombre, marca o cualquier otro signo distintivo en el producto (art. 3.1). Junto a éste merecen la consideración de fabricante el importador (art. 3.2) y el suministrador a no ser que informara al perjudicado de la identidad del productor o de la persona que le suministró el producto dentro de un plazo de tiempo razonable (art. 3.3).

Si se hace recaer exclusivamente en el fabricante la responsabilidad cuando el defecto no es propiamente de fabricación y, además, en el diseño, por ejemplo, han intervenido varias personas identificadas individualmente (v. gr. creador del algoritmo, programador, diseñador, fabricante de alguna pieza, ...) o bien grupo o equipo de investigación, puede existir cierta falta de interés en invertir en la fabricación sistemas de IA. Por otro lado, este concepto amplio de productor recogido en la norma comunitaria es un concepto que ha sido calificado de estático, lineal relativo a la cadena de producción de productos tangibles, alejado de la realidad del mercado digital, en el que intervienen otros operadores, tales como las plataformas intermediarias²⁹ o, en la economía circular, los empresarios que reparan, rehabilitan o recomponen los productos, los cuales pueden ser los mismos que los fabricaron como otros autorizados por éstos³⁰. Y en el que hay un constante flujo de datos desde el consumidor al fabricante o a otros intervinientes y viceversa en la cadena de producción (*co-generated data*).

Si se considera que gran parte de defectos, en caso de sistemas de IA, puedan provenir de defectos de diseño o de concepción

²⁸ DOUE L169/1, 25.06.2019. *ELI Draft of a Revised Product Liability Directive*, p. 11.

²⁹ *ELI Draft of a Revised Product Liability Directive*, p. 18.

³⁰ V. MAK / E. TERRY, “Circular Economy and Consumer Protection: The Consumer as a Citizen and the Limits of Empowerment Through Consumer Law”, *J. Consum. Policy* (2020) 43:227-248, p. 236.



Foto de Cottonbro en Pexels.



podría ampliarse el concepto de “productor” incorporando al “ingeniero diseñador”³¹, siempre que sea un tercero ajeno a la esfera del primero, es decir, no trabaje para él. En el Informe del grupo de expertos de alto nivel el “diseñador” del sistema puede ser considerado uno de los “operadores”, en particular, podría ser “*backend operator*”.

De todos modos, en la medida en que el sistema de IA se considere una parte integrante del “producto”, y, además, esencial, el fabricante del producto final podrá verse exonerado de responsabilidad si el defecto se debe al diseño de un elemento componente, siéndolo en este caso, el sistema de IA. Así, el diseñador de éste podría responder directamente en cuanto “fabricante de un elemento integrante” del sistema de IA por los daños ocasionados (art. 7 letra f Directiva 85/374/CEE). Ahora bien, si se amplía el concepto de “producto” incluyendo, como he indicado, a los bienes con elementos digitales, sería posible que la víctima se pudiera dirigir directamente al fabricante del producto acabado también por los defectos que presentara el elemento digital cuando éste es esencial para el funcionamiento de aquél sin necesidad de que tenga que ejercitar acciones contra el tercero que suministró el elemento digital. Como entre fabricante del producto acabado y este tercero existe una relación contractual, las cuestiones de responsabilidad se solventarán en ese ámbito³².

5. Daños

Como es conocido, el art. 9 Directiva 85/374/CEE (art. 129.1 TRLGDCU) describe qué se entiende por daños: a) los daños causados por muerte o lesiones corporales; b) los daños causados a una cosa o la destrucción de una cosa, que no sea el propio producto defectuoso, previa deducción de una franquicia de 500 euros³³, a condición de que tal cosa: i) sea de las que normalmente se destinan al uso o consumo privados y ii) el perjudicado la haya utilizado principalmente para su uso o consumo privados.

No se contemplan, en cambio, daños psicológicos, los daños a bienes digitales o a datos ya sean los derivados de la operación de que se trate como a otros datos titularidad de la víctima³⁴. Además, muchos bienes tienen un propósito mixto, esto es, privado y profesional a un tiempo como sucede en el supuesto del uso por los *prosumidores* de impresoras 3D para producir bienes, en su ámbito privado, que luego comercializan³⁵ o en el ámbito del teletrabajo. A este respecto puede recordarse el considerando núm. 17 de la Directiva 2011/83/UE, de 25 de octubre, sobre derechos de los consumidores³⁶, en el que se indica, acerca de la definición actual de “consumidor”, que “debe incluir a las personas físicas que actúan fuera de su actividad comercial, empresa, oficio o profesión.

³¹ *ELI Draft of a Revised Product Liability Directive*, p. 12. Siguiendo esta línea, vid. M.^a L. ATIENZA NAVARRO, *Daños causados por inteligencia artificial*, pp. 154-157.

³² *ELI Reponse to the public consultation on civil liability*, p. 11.

³³ Debería eliminarse este límite pues se ha comprobado en el seguimiento de la aplicación de la misma en las legislaciones nacionales que no ha resultado eficaz (*ELI Draft of a Revised Product Liability Directive*, p. 15).

³⁴ *ELI Draft of a Revised Product Liability Directive*, p. 13.

³⁵ Ch. TWIGG-FLESNER, “Guiding Principles”, p. 5.

³⁶ DOUE L 304/64, 22.11.2011. Vid. la STJUE de 20 de enero de 2005, C-464/10.

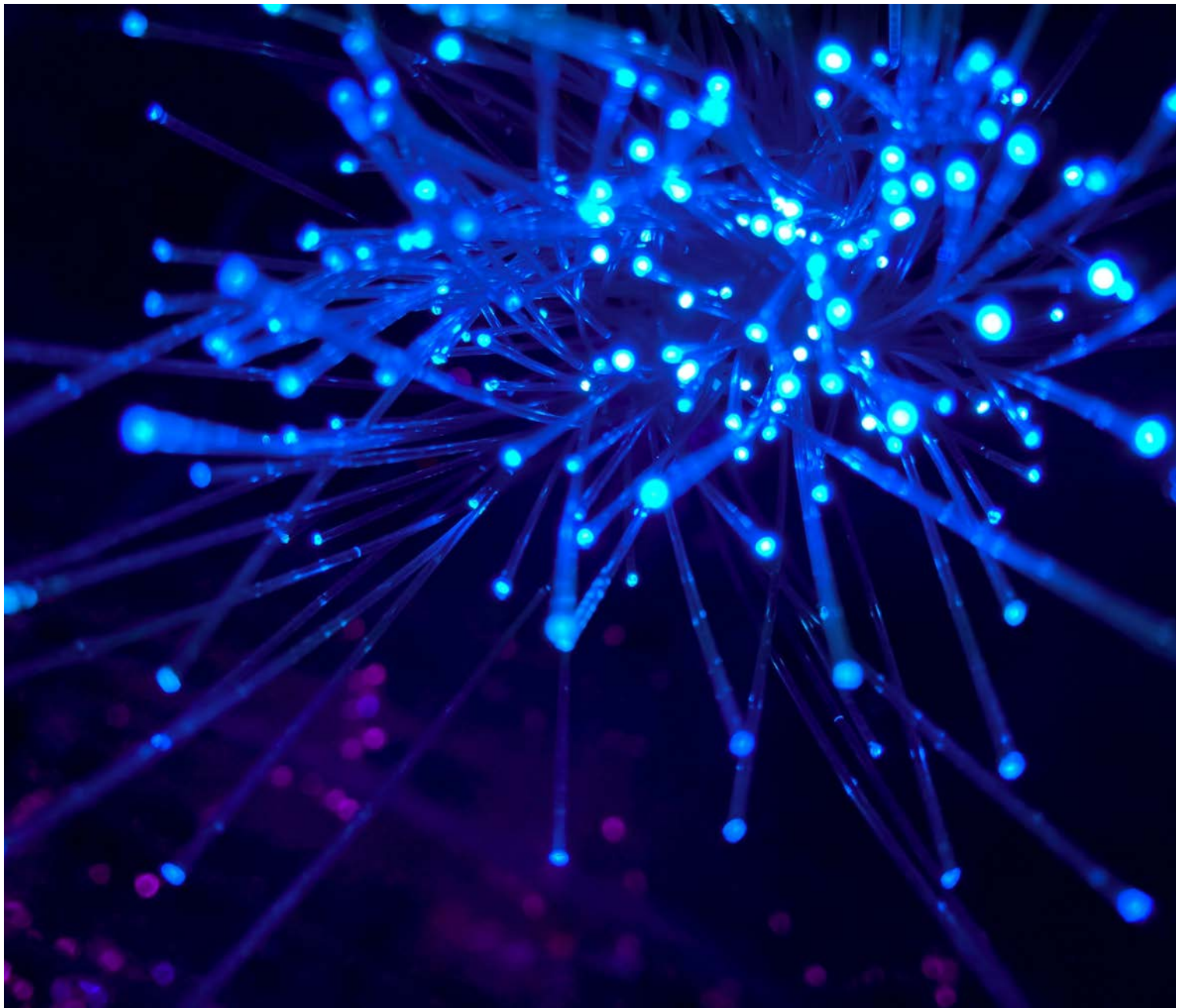


Foto de JJ Ying en Unsplash.

No obstante, en el caso de los contratos con doble finalidad, si el contrato se celebra con un objeto en parte relacionado y en parte no relacionado con la actividad comercial de la persona y el objeto comercial es tan limitado que no predomina en el contexto general del contrato, dicha persona deberá ser considerada como consumidor”. En mi opinión, éste es un aspecto que también se debería contemplar en la futura reforma de la Directiva 85/374/CEE. Quizá, como propone la revisión de la Directiva elaborada por el ELI, debería incluirse a los profesionales³⁷.

6. Carga de la prueba para la víctima

En relación con la carga de la prueba ya se conocen las dificultades que existen, para la víctima, en cuanto a la prueba del nexo causal y del defecto en caso especialmente de bienes digitales o de bienes tangibles con elementos digitales. Eso ha hecho que la jurisprudencia emplee diferentes mecanismos jurídicos, así como medios de prueba para aliviar la carga de la prueba a la víctima. En todo caso, el daño debe probarlo la víctima.

Las recomendaciones del Grupo de expertos en responsabilidad civil y nuevas tecnologías en relación con los diversos expedientes para facilitar la prueba a la víctima, ora del defecto,

del nexo causal o de la culpa son perfectamente aplicables al caso que me ocupa.

El Informe, 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*.

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.

En esta materia deberían existir normas idénticas puesto que la problemática que genera el IoT³⁸, la puesta en circulación o en servicio de un sistema de IA que interactúa comunicándose en el mercado con otros sistemas de IA, que pueden o no ser elementos componentes de bienes corporales, es esencial-

³⁷ ELI Draft of a Revised Product Liability Directive, p. 15.

³⁸ ELI Reponse to the public consultation on civil liability, p. 18.

mente la misma. En relación con este aspecto, las consideraciones del Grupo de expertos acerca de las “unidades comerciales y tecnológicas” son especialmente interesantes y deberían apoyarse en una futura reforma de la Directiva que trato³⁹. En este sentido, se ha advertido la necesidad de expandir el ámbito de aplicación del art. 4 de la Directiva 85/374/CEE para incluirlas.

IV. CONCLUSIÓN

La IA y las tecnologías emergentes están propiciando una importante modificación del régimen legal de la responsabilidad civil con una tendencia clara a criterios basados en el riesgo. Así, paulatinamente profesiones en las cuales el criterio de imputación de la responsabilidad se ha venido basando en la falta de diligencia debida desde el momento

en que intervenga un sistema de IA que pueda considerarse de alto riesgo pasarán, en caso de daños, a estar basadas en la deficiente gestión del riesgo. Aún así cuando el sistema manejado sea de bajo riesgo la responsabilidad por los daños ocasionados no será una responsabilidad por culpa –digamos– “pura”. El caso paradigmático es –será– el de la profesión médica. La existencia de un régimen general con otros sectoriales se antoja la solución más oportuna en esta materia.

Por otra parte, como advertía, deberá pensarse muy bien el régimen de compatibilidad entre la posible Propuesta de reglamento que salga a partir de las recomendaciones del Parlamento europeo realizadas en 2020 con la revisión de la Directiva 85/377/CE para evitar que se rebaje el nivel de protección de los consumidores de suerte que determinados defectos en productos queden apartados del régimen de responsabilidad objetiva de esta norma comunitaria para quedar comprendidos en el régimen de responsabilidad por culpa, aunque sea culpa “objetivizada”, establecido en el futuro reglamento de responsabilidad civil por el uso de sistemas de IA. ♦

³⁹ Expert Group on Liability and New Technologies (NTF), “Liability for AI and other emerging digital technologies”, pp. 49, núms. 29-30 (nota a pie de página n.º 2); C. TWIGG-FLESNER, “Guiding Principles”, p. 7.

Novedad

DERECHO PRIVADO ROMANO

Undécima edición

ANTONIO FERNÁNDEZ DE BUJÁN

ISBN: 978-84-9890-435-2. Págs.: 616. 49,5 € IVA incluido

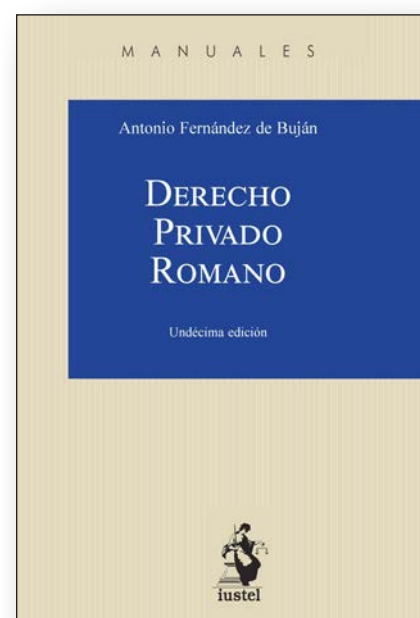
La experiencia iusprivatística romana constituye una manifestación clásica de la ciencia del derecho, que trasciende el periodo de tiempo en que se produce, para conformar el pilar básico sobre el que se asienta el derecho privado continental europeo. La mayoría de los conceptos, instituciones, reglas y soluciones a las cuestiones, así como la sistemática que informa el actual ordenamiento jurídico, en materia de derecho privado, tienen su origen en el Derecho romano. Roma inventa el Derecho en Occidente, y ensambla por vez primera, en expresión orteguiana, el oriente y el occidente de Europa. El Derecho romano constituye la experiencia jurídica más paradigmática de la historia europea. La enseñanza del Digesto justiniano en la Bolonia del siglo xi, está en el origen de la que fue la primera universidad europea y contribuye, desde entonces, a la conformación de la lógica jurídica de los estudiantes de las Facultades de Derecho.

El estudio del Derecho privado romano, constituye no sólo un elemento indispensable para valorar la historicidad del Derecho, sino que también se configura como un instrumento necesario para entender el derecho vigente y para ayudar a la construcción, sobre los elementos comunes que el Derecho romano proporciona a los Códigos civiles europeos, del derecho privado de la Unión Europea, que el irreversible proceso unificador nos deparará en el futuro.

El Autor del presente Manual, Catedrático de Derecho Romano de la Universidad Autónoma de Madrid, parte de la consideración del Derecho como un producto histórico, idea fuerza que informa el contenido de su obra, en la que pone de manifiesto, en cada uno de los capítulos que la componen, la concordancia, entre las soluciones que se dan en el Derecho Romano, a las distintas cuestiones que se plantean, y las previstas en un número importante de artículos del vigente Código Civil español, paradigma legislativo, que se conforma como el último eslabón de la evolución del pensamiento jurídico, desde Roma hasta el actual derecho positivo español.

Constituye el objeto de estudio de esta valiosa aportación a la ciencia del derecho, que publica la Editorial Iustel, el análisis del derecho procesal, el derecho de la persona, el derecho de familia, el negocio jurídico, los derechos reales, el derecho de obligaciones y el derecho contractual.

Se ha procedido, en esta undécima edición, a revisar el contenido íntegro de la obra y a actualizar el índice analítico.



Para más información www.iustel.com