DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

7

INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

Itziar Alkorta Idiakez
Cristina Argelich Comelles
Maria Cristina Berenguer Albaladejo
Yolanda Bustos Moreno
Maria Raquel Evangelio Llorca
Beatriz Extremera Fernández
Pedro José Femenía López
María Remedios Guilabert Vidal
María Jorqui Azofra
Raúl Lafuente Sánchez
Pedro José López Mas
Raquel Luquin Bergareche
Andrés Marín Salmerón
Luz Martínez Velencoso
Lucía Molina Martínez
Óscar Monje Balmaseda
Esther Monterroso Casado
Juan Antonio Moreno Martínez
Carmen Muñoz García
Alberto Muñoz Villarreal
Íñigo Navarro Mendizábal
Manuel Ortiz Fernández
Miquel Peguera Poch
Antonio Rubí Puig
Alberto Tapia Hermida

Dykinson, S.L.

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

INTELIGENCIA ARTIFICIAL
Y DERECHO DE DAÑOS:
CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

COLECCIÓN
DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

Moreno Martínez, J.a.
Femenía López, P.j.
(Coordinadores)

Itziar Alkorta Idiakez
Cristina Argelich Comelles
Maria Cristina Berenguer Albaladejo
Yolanda Bustos Moreno
Maria Raquel Evangelio Llorca
Beatriz Extremera Fernández
Pedro José Femenía López
María Remedios Guilabert Vidal
María Jorqui Azofra
Raúl Lafuente Sánchez
Pedro José López Mas
Raquel Luquin Bergareche
Andrés Marín Salmerón
Luz Martínez Velencoso
Lucía Molina Martínez
Óscar Monje Balmaseda
Esther Monterroso Casado
Juan Antonio Moreno Martínez
Carmen Muñoz García
Alberto Muñoz Villarreal
Íñigo Navarro Mendizábal
Manuel Ortiz Fernández
Miquel Peguera Poch
Antonio Rubí Puig
Alberto Tapia Hermida

Dykinson, S.L.

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial.
Para mayor información, véase *www.dykinson.com/quienes_somos*

Este trabajo se enmarca en el Proyecto I+D+i (Referencia: PID2020-116185GB-100) del Ministerio de Ciencia e Innovación: "La irrupción de la inteligencia artificial en el Derecho de Daños y su adaptación a las nuevas tecnologías", siendo investigadores principales los profesores Juan Antonio Moreno Martínez y Pedro José Femenía López.

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69
e-mail: info@dykinson.com
http://www.dykinson.es
http://www.dykinson.com

ISBN: 978-84-1070-708-5
Depósito Legal: M-25437-2024
DOI: https://doi.org/10.14679/3532

ISBN electrónico: 978-84-1122-801-5

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

Índice

La armonización del tratamiento legal de la responsabilidad civil contractual y extracontractual del metaverso con la regulación europea sobre plataformas en línea

Cristina Argelich Comelles

Profesora Ayudante Doctor de Derecho civil
Universidad Autónoma de Madrid

1. CONSIDERACIONES INICIALES ACERCA DEL METAVERSO Y LA RESPONSABILIDAD CIVIL

Para abordar la naturaleza jurídica del Metaverso, un acrónimo formado por el prefijo "meta-", que significa más allá, y el sustantivo "universo", no

encontramos un concepto actual y completo del Metaverso, que integre el *hardware* y su interacción entre la realidad digital y el mundo real. Por ello, definimos el Metaverso como la red de mundos virtuales en tres dimensiones, a modo de traslación de Internet al mundo real como realidad digital, y centrados en la conexión social con el usuario mediante su *hardware:* la realidad aumentada -y su interacción con auriculares y gafas de realidad aumentada-, la realidad mixta, la realidad virtual, y las tecnologías de la realidad digital[1]. Estas se componen de: la tecnología *blockchain,* para la automatización de las decisiones previamente programadas; Web3 o el Internet operado mediante tecnología *blockchain*, cuyo contenido es inmutable e incensurable, y no se puede hackear ni colgar; y los sistemas de inteligencia artificial o IA para la toma autónoma de decisiones.

En consecuencia, la naturaleza jurídica que le corresponde al Metaverso es la propia de la Tierra virtualizada como realidad digital, porque a ella se vincula, aunque pueda operar paralelamente. Calificarla así permite que los abusos tengan el tratamiento legal propio de la realidad material, con las adaptaciones que requiera para su aplicación en este entorno digital, algo especialmente relevante en materia de responsabilidad civil extracontractual por los daños causados en el Metaverso. La tecnología que requiere el Metaverso se compone del *hardware,* como la realidad aumentada, la realidad mixta y la realidad virtual, junto con las tecnologías de la realidad digital, consistentes en la tecnología *blockchain* y Web3, así como el *software* pertinente.

Hechas estas precisiones iniciales y por lo que respecta a la estructura del presente trabajo, se analizará la propiedad de los activos digitales alojados en las plataformas en línea, también las del Metaverso, como son un ejemplo los *in-game digital assets,* para seguidamente abordar la identidad digital del responsable civil. Tras ello, se examinará el régimen de responsabilidad del proveedor de servicios de la plataforma en línea y del usuario profesional en el ordenamiento jurídico europeo para incardinar posteriormente la responsabilidad civil contractual por incumplimiento, debiendo destacar la pérdida o desprogramación de los activos digitales y por discriminación algorítmica como ejemplos de la insuficiencia del régimen de responsabilidad actual, y la responsabilidad civil extracontractual por los daños causados en el Metaverso.

---

[1] ARGELICH COMELLES, C. (2022). El Derecho civil ante el Metaverso: hacia un Metalaw europeo y sus remedios en el Multiverso. *Derecho digital e innovación,* 12, 1-26.

2. IDENTIDAD DIGITAL DEL RESPONSABLE CIVIL Y PROPIEDAD DE LOS ACTIVOS DIGITALES PATRIMONIALES

Tras la aprobación del Reglamento 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE[2], conocido como eIDAS, se ha evolucionado de la firma electrónica a la identidad digital con el Reglamento 1183/2024 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital[3]. La identidad digital va a facilitar la mejora de la seguridad en la autenticación en las plataformas en línea. Además, permitirá enlazar dicha identidad digital a la representación gráfica del usuario y, por ende, vincularle el régimen de responsabilidad civil correspondiente. No obstante, el principal reto jurídico se sitúa en el tratamiento legal del procesamiento automático de los datos de carácter personal[4], en atención al régimen de responsabilidad por dicho procesamiento ilegal de datos, fijado por el Tribunal de Justicia de la Unión[5].

En el ámbito de la Unión Europea, los criptoactivos encuentran su regulación en el Reglamento 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos 1093/2010 y 1095/2010 y las Directivas 2013/36/UE y 2019/1937[6], conocido como Reglamento MiCA, que establece obligaciones para los emisores y proveedores de servicios de criptoactivos, así como en la regulación establecida para los mercados e instrumentos financieros en la Directiva MiFID II y el Reglamento MiFIR. En este sentido, encontramos diversos tipos de criptoactivos que examinaremos[7], a saber: las criptomonedas, las *stablecoins* y las divisas digitales controladas por un Banco Central; los

---

[2] DOUE de 28 de agosto de 2014.

[3] DOUE de 30 de abril de 2024.

[4] WALSHE, P. (2020). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention 108. Digital Identities. Council of Europe, 1-24, https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc-en/1680a0c051.%20/.

[5] STJUE de 5 de marzo de 2024, ECLI:EU:C:2024:202.

[6] DOUE de 9 de junio de 2023. FETSYAK SENKIV, I. (2024). Impacto de la Propuesta de Reglamento de prevención de blanqueo de capitales en las transacciones con criptoactivos. ¿El fin de las «wallet» sin custodia y de las transacciones «crypto» anónimas?, *Diario La Ley,* 10487, 1-5.

[7] KRYSA, F. (2023). Taxonomy and Characterisation of Crypto Assets in Private International Law. En BONOMI, A., LEHMANN, M., LALANI, S., (eds.), *Blockchain and Private International Law,* Leiden, Brill, 157-208. PARRONDO, L. (2023). Cryptoassets: Definitions and accounting treatment under the current International Financial Reporting Standards framework. *International Journal of Intelligent Systems in Accounting and Finance Management,* 4, 1-20.

tokens no fungibles; y los *security tokens,* vinculados a inversiones financieras o a la Tokenización de bienes u otros activos.

En primer lugar, las criptomonedas son instrumentos de pago carentes de soporte físico, que se basan en un algoritmo y el registro electrónico donde se almacenan. Es necesario precisar que se trata de un algoritmo matemático, como lo son la mayoría, y que no está entrenado con Inteligencia Artificial a los efectos de que su funcionamiento sea cambiante, como sucede en los *dynamic pricing algorithms,* por ejemplo. Encontramos también las *stablecoins,* es decir, una criptomoneda de cotización estable y cuya operatividad radica en la facilitación de pagos e intercambios en el extranjero, evitando las variaciones en los tipos de cambio por los pagos en divisas diferentes. Para concluir con los criptoactivos, es necesario referirse a las *Central bank digital currencies,* conocidas como CBDCs, y referidas a una moneda digital que representa la divisa controlada y emitida por un Banco Central, como lo será en un futuro el Euro digital o EURM, que actualmente está en fase de pruebas.

En segundo lugar, encontramos los *non-fungible tokens* o NFTs, es decir, un token que representa la propiedad de un activo digital único e individualizado -por tanto, no fungible y cuya transmisión se sujeta al régimen jurídico de las obligaciones específicas-, a modo de certificado al *tokenholder* como propietario y que le faculta para su disposición. Asimismo, el token en los NFTs también puede utilizarse para probar la identidad de su titular, para tokenizar la transmisión de la propiedad con trazabilidad de la operación, así como para probar la propiedad de ítems virtuales en videojuegos y plataformas en línea, como los avatares -tokenizados-, las fincas virtuales o los *in-game digital assets.* Separadamente, encontramos los *security tokens,* utilizados como ficha de seguridad para una inversión financiera, como acciones o bonos, así como obras de arte[8], y también para la Tokenización de activos reales o digitales.

Habida cuenta de lo expuesto, los activos digitales se programan de la siguiente manera: la representación gráfica es *online,* y la programación de sus metadatos se encuentra *on-chain*. Por tanto, los activos digitales no tienen un activo real vinculado, lo que incide en su tratamiento legal respecto de la Tokenización de bienes[9]. A modo de ejemplo divulgativo, la representación gráfica y los metadatos de los NFTs corresponderían a un objeto y su código de

---

[8] LACRUZ MANTECÓN, M. L. (2023). Propiedad Intelectual y tecnología inteligente. *Revista Crítica de Derecho Inmobiliario,* 99(800), 3103-3146.

[9] NASARRE AZNAR, S. (2020). Naturaleza jurídica y régimen civil de los "tokens" en "blockchain". En GARCÍA TERUEL, R. M. (coord.), *La tokenización de bienes en blockchain: cuestiones civiles y tributarias,* Cizur Menor, Thomson Reuters Aranzadi, 61-108. GARCÍA-TERUEL, R. M., SIMÓN-MORENO, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review,* 41, 1-16. ARRIETA SEVILLA, L. J. (2023). El uso de tokens en transmisiones inmobiliarias. *Revista de Derecho Civil,* X(2), 71-116.

barras en la realidad material, respectivamente. Un código de barras permite la identificación del bien, pero no impide su transformación no autorizada, ni la pérdida de la cosa debida o la imposibilidad sobrevenida de la prestación; en el entorno digital, este último supuesto tendrá lugar mediante la desprogramación del activo digital. En consecuencia, debido a su existencia *online* y *on-chain,* lo único que es posible trasladar de un activo digital a la realidad material es el almacenamiento de una copia de su representación gráfica, como archivo, no como activo, y cuya calificación jurídica será la de dato.

Respecto del uso de los activos digitales patrimoniales en la realidad material[10], los criptoactivos se podrán utilizar remotamente mediante las *cryptowallets,* a modo de cartera virtual. En este sentido, las criptomonedas son aceptadas como método de pago en diversas plataformas en línea, e incluso cabe canjear su saldo disponible en métodos de pago como *PayPal,* en este caso, respecto de la criptomoneda *Bitcoin*. Por otra parte, los *NFT wallets* permiten almacenar la información sobre la ubicación de los NFTs en la plataforma donde se alojan los metadatos, así como adquirir nuevos NFTs, al tiempo que aseguran la interoperabilidad agrupando los NFTs coleccionables ubicados en diversas plataformas.

3. EL RÉGIMEN DE RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE LA PLATAFORMA Y DEL USUARIO PROFESIONAL EN EL ORDENAMIENTO JURÍDICO EUROPEO

El régimen jurídico de las plataformas en línea, también aplicable a las que conforman el Metaverso, se distribuye en diversos Reglamentos europeos, a saber: el Reglamento 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea[11], en adelante, *P2B Regulation;* el Reglamento 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales[12]), en adelante, DSA; y el Reglamento 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre merca-

---

[10] SCHULLER, R. R. (2022). Criptoactivos. Categorización jurídica de los criptoactivos e introducción a la tecnología DLT/Blockchain. *Cuadernos de Derecho Transnacional,* 14(2), 737-769. PACHECO JIMÉNEZ, M. N. (2022). De la digitalización de los pagos a los tokens del metaverso. *La Ley mercantil,* 91, 1-20.

[11] DOUE de 11 de julio de 2019.

[12] DOUE de 27 de octubre de 2022.

dos disputables y equitativos en el sector digital y por el que se modifican las Directivas 2019/1937 y 2020/1828 (Reglamento de Mercados Digitales[13]), en adelante, DMA.

En el estudio elaborado para el Parlamento Europeo, de 5 de febrero de 2021, denominado *Liability of online platforms*[14], se examinan las principales alternativas regulatorias ante la responsabilidad de las plataformas en línea: mantener el estado de la cuestión; la sensibilización acerca de su utilización; la promoción de la autorregulación; el establecimiento de herramientas de corregulación; la adopción de normativa estatutaria sobre la responsabilidad de las plataformas; y la modificación de la responsabilidad de las plataformas en línea, mediante las condiciones para la exención de responsabilidad o el establecimiento de un régimen armonizado de responsabilidad.

A este respecto, es oportuno indicar que los algoritmos no son neutrales, pues algunos utilizan la IA, como lo relativos al *pricing,* y su programación puede tener sesgos humanos. Todo ello conduce a un eventual resultado discriminatorio en la elección final del consumidor en las plataformas en línea. En el ámbito de las plataformas en línea, la discriminación algorítmica puede producirse de diversas maneras[15], pues la formación del algoritmo se divide en tres fases: *process level, model level* y *classification level*. En la fase *process level,* el *machine learning* mediante el que el algoritmo se forma y adapta al entorno puede contener datos sesgados, que alteren materialmente su neutralidad teórica. En la fase *model level,* ello obedece a que los datos originarios son parciales o incorrectos, lo que se soluciona mediante un tratamiento de datos adecuado del *Big Data;* esto es, lo que se conoce como *cleaning the data*, o que dichos datos se encuentren vinculados a una discriminación estructural. En la fase *classification level,* ello sucede cuando, en la selección de unas determinadas características del consumidor o factores relativos al producto, se ocasiona la discriminación que la propia plataforma pretende, por ejemplo, porque el *target* de clientes de un determinado producto deba reunir unas características. En el Derecho del consumo no disponemos, ni en los Estados Unidos ni en el Derecho de la Unión, de una regulación relativa a la discriminación algorítmica que articule remedios para mitigar sus efectos.

---

[13] DOUE de 12 de octubre de 2022.

[14] EUROPEAN PARLIAMENT (2021). *Liability of online platforms,* European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf.

[15] WHITTAKER, M., CRAWFORD, K., DOBBE, R., FRIED, G., *et. al.* (2018). *AI Now Report,* European Commission, Futurium, 1-63, ttps://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf. KROLL, J., HUEY, J., BAROCAS, S., FELTEN, E., *et. al.* (2017). Accountable Algorithms. *University of Pennsylvania Law Review,* 165, 633-705, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

Por todo ello, mientras no se aborde una regulación en materia de discriminación algorítmica omnicomprensiva, tendremos que encomendarnos a la autorregulación de las plataformas en línea mediante los mecanismos reputacionales, así como los eventuales *Corporate Compliance* de las empresas a las que se vinculan, para atender materialmente la protección del consumidor en este ámbito. Así, será posible proporcionar información acerca del tratamiento de los datos vertidos en la plataforma, la información de los derechos acerca de su tratamiento, las obligaciones de la plataforma al respecto, el acceso a los mismos y su confidencialidad, y las acciones de los poderes públicos al respecto. No obstante, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[16] -en adelante RGPD- solo se refiere a datos de carácter personal; ello excluye el *machine learning* y los datos personales que sean necesarios para evitar la discriminación en las materias en las que ha sido regulada. En suma, la regulación algorítmica omnicomprensiva que debería abordarse pasa, de momento, por la autorregulación en las plataformas en línea.

Por lo que respecta al régimen jurídico aplicable a las plataformas en línea, analizaremos brevemente los Reglamentos europeos indicados. El examen de la *P2B Regulation* tendrá carácter tangencial, por referirse a la relación jurídica entre una plataforma y un empresario, por tanto, B2B; en este caso, entre un usuario profesional respecto de una plataforma intermediaria en línea, habitualmente bajo la figura del contrato de distribución. Sin embargo, su importancia es indubitable, pues constituye el primer antecedente normativo para pasar de la autorregulación de las plataformas a su normativización en el contexto del mercado único europeo. Respecto de los algoritmos y la protección del consumidor, se encuentra una referencia expresa a los algoritmos en el art. 5.6: a los efectos de establecer los parámetros principales que rigen la clasificación de los productos o servicios en las plataformas en línea, no se exigirá a los proveedores de los servicios de intermediación en línea ni a los proveedores de los motores de búsqueda la revelación de los algoritmos que puedan inducir a error a los consumidores, o bien causarles un perjuicio mediante la manipulación de los resultados.

En cuanto a la prevención de la discriminación algorítmica en los contratos de consumo, la DSA se fundamenta en tres objetivos específicos en el art. 1: la protección efectiva de los consumidores y sus derechos fundamentales en las plataformas en línea; el establecimiento de la transparencia y responsabilidad de estas plataformas; y la promoción de la innovación, el crecimiento y la

[16] DOUE de 4 de mayo de 2016.

competitividad en el mercado único europeo. La *P2B Regulation* se enfoca en la transparencia y los remedios privados en las relaciones B2B, mientras que la DSA atribuye responsabilidad al proveedor de la plataforma cuando preste el servicio, salvo por las causas de exoneración de los arts. 4-6, como hemos explicado. Complementariamente, se ha creado el Observatorio de la Unión Europea sobre la economía de las plataformas en línea para examinar las últimas tendencias en este tema, en relación con la Recomendación de la Unión Europea 2018/334, de 1 de marzo de 2018, sobre medidas para abordar de manera efectiva los contenidos ilegales en línea, también regulada en el art. 8 DSA.

La DSA confirma el principio de responsabilidad limitada de los intermediarios en línea, pues no se produce una ampliación de la responsabilidad civil. El fundamento de este régimen de responsabilidad se encuentra en las *asymmetric due diligence obligations* u obligaciones asimétricas de diligencia debida que deben cumplir las autoridades competentes. Las obligaciones de diligencia debida se sustentan, a su vez, en la transparencia y el *platform procedure* o procedimiento de plataforma, como por ejemplo la notificación y tramitación de reclamaciones, la solución extrajudicial de controversias, los mecanismos reputacionales e incluso la incorporación del *Corporate Compliance*. Con este enfoque en cuestiones de procedimiento, la DSA sigue la tendencia reciente de una "procedimentación" de la regulación de la plataforma, como se había venido produciendo mediante la autorregulación con los mecanismos reputacionales, así como en la *P2B Regulation*. En este sentido, debemos mencionar que en las *Model Rules on Online Platforms*[17] del *European Law Institute* se incide en las cuestiones clave en materia de responsabilidad de las plataformas en línea, como son la falta de transparencia, la influencia de la plataforma sobre el proveedor y la falta de diligencia. Finalmente, para las *very large online platforms* o grandes plataformas en línea, el art. 33 DSA aporta una nueva forma de regulación sectorial para plataformas sistémicamente importantes. Este enfoque se basa en la regulación de los servicios financieros con diversas obligaciones de cumplimiento. Deberemos atender a si las obligaciones de presentación de informes y auditoría son suficientes para garantizar un "entorno en línea seguro, confiable y transparente", como exige la DSA.

En cuanto a la DMA, el objetivo es conseguir que las plataformas en línea de gran tamaño actúen de forma justa en su actividad, con los criterios objetivos de su calificación como guardián de acceso contenidos en los arts. 1 y 3: tener una posición económica sólida, un impacto significativo en el mer-

[17] EUROPEAN LAW INSTITUTE (2019). *Model Rules on Online Platforms,* https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

cado interior y estar activo en varios Estados de la Unión Europea; tener una fuerte posición intermediaria al vincular una pluralidad de usuarios a diversas empresas; y tener una posición consolidada en el mercado. La DMA garantiza la equidad de los términos y condiciones de las plataformas en línea al establecer las prácticas comerciales desleales de los guardianes de acceso en su art. 5. La DMA también mejora la oferta al consumidor y permite que las plataformas se ocupen de nuevos servicios. En caso de incumplimiento de las normas establecidas, se establece un régimen sancionador de hasta el 10% de la facturación anual de la empresa, así como otros remedios y sanciones tras una investigación de la plataforma. Finalmente, el tratamiento legal de la transparencia algorítmica en la DMA se concreta en su examen y el régimen de responsabilidad, el papel de los algoritmos en la economía y sociedad digital junto con la gobernanza de datos, así como los códigos de conducta, en relación con el *Corporate Compliance* y los mecanismos reputacionales.

3.1. La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad civil contractual: hacia un sistema de responsabilidad civil objetiva por pérdida o desprogramación de un activo digital y por discriminación algorítmica

A los efectos de apreciar la pérdida o destrucción de la cosa, los activos digitales no se pueden deteriorar, sino que solamente se pueden desprogramar de la plataforma donde se almacenen sus metadatos. Dicha desprogramación obedecerá a dos causas: por el cumplimiento de las obligaciones establecidas en la normativa europea sobre plataformas en línea, o bien por un "hackeo" o ataque informático al registro electrónico que contiene los metadatos del activo digital. Por una parte, la desprogramación del proveedor de servicios de la plataforma en línea, en cumplimiento de las obligaciones de suspensión y terminación del servicio de un usuario profesional en caso de afectación a los derechos de terceros, en virtud de los arts. 4 y 5 de la *P2B Regulation*-, le exoneran de responsabilidad en los arts. 4-6 DSA, siendo responsable el usuario profesional frente al titular o consumidor del activo digital.

Respecto de la pérdida del activo digital en atención a lo expuesto, conviene referir el caso "Metabirkins" o la transformación no autorizada en NFTs del bolso *Birkin* de la firma *Hermès* por parte del usuario profesional *Metabirkins,* así como su comercialización indebida en diversas plataformas en línea. En el caso *Hermès Int'l v. Rothschild*, enjuiciado por el Tribunal Federal de Nueva York el pasado 2 de febrero de 2023, se establece que dicha comercialización correspondería a la firma *Hermès* o mediante su transformación autorizada,

por lo que condenó a la parte demandada a pagar 130.000 dólares en concepto de indemnización por daños y perjuicios[18]. Por otra parte, la pérdida del activo digital puede producirse por un "hackeo" o ataque informático, quedando el proveedor de la plataforma habilitado para reprogramar el activo digital. El "hackeo" ocasiona un *bug* o falla en la *blockchain* que hace que no se pueda autoejecutar lo programado, por lo que el único remedio informático es la reprogramación desde el *hash* anterior a este *bug*, para que así se autoejecute la cadena más larga. Los casos de los *crypto panics* ilustran bien lo expuesto, pues cuando se produce dicho ataque informático, la única solución es su reprogramación.

Complementariamente y en materia de errores de programación y hackeos, el *MIT Media Lab*[19] señala que los *hackers* se han apropiado del equivalente a 1.800 millones de dólares en criptomonedas. Ello se debe a los *bugs* o errores en el programa informático de las plataformas correspondientes. En particular, no referimos a los fallos en la plataforma *Ethereum,* conocidos como el ataque a *The DAO*[20] de 2016 y el ataque a *Parity*, junto con otros casos a los que nos remitimos[21]. Estos errores en la programación derivan del automatismo de la tecnología *blockchain* y, en consecuencia, de su irreversibilidad, porque no se puede detener su ejecución sino solamente revertir sus efectos mediante la reprogramación. Ningún código informático está exento de *bugs,* lo que requiere su comprobación previa en aras de evitar resultados inadecuados y garantizar su ejecución sin intervención humana o reprogramación. Estos errores conllevan el incremento de la inversión para evitarlos y de los costes de indemnización por una programación defectuosa. Por ello, apuntamos que una extensión del Metaverso mediante las plataformas en las que opera debería llevar aparejada una responsabilidad de carácter objetivo de la plataforma, mediante la aceptación de los términos y condiciones de uso de esta, siendo especialmente útil en caso de un error de programación en la plataforma. Asimismo, dicha aceptación debería llevar aparejada la formaliza-

---

[18] Hermes Int'l v. Rothschild, 22-cv-384 (JSR) (S.D.N.Y. Feb. 2, 2023), https://casetext.com/case/hermes-intl-v-rothschild-9. Cuestión distinta es el reciente y sorprendente pronunciamiento acerca de la creación de NFTs sobre obras pictóricas, cuyo titular es la firma Mango, en el que se ha autorizado la transformación en estos activos digitales aun no siendo esta firma la autora de las obras pictóricas. Véase la SJM Barcelona de 11 de enero de 2024, ECLI:ES:JMB:2024:1.

[19] ORCUTT, M. (2019). Once hailed as unhackable, blockchains are now getting hacked. *MIT Technology Review,* https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

[20] ATZEI, N., BARTOLETTI, M., CIMOLI, T. (2017). A survey of attacks on Ethereum smart contracts. *Proceedings of the 6th International Conference on Principles of Security and Trust,* 10204, 1-23.

[21] Estos casos se refieren a *CoinDash ICO*, con una pérdida en criptomonedas de 10 millones de dólares, la Estafa del Proyecto Enigma, consistente en una preventa falsificada de *Tokens* que supuso una pérdida de 1.500 *Ethers*, el robo de *Tether,* que perdió el equivalente a 31 millones en *Tokens*, y la Estafa de Bitcoin Gold, que conllevó una pérdida del equivalente a 3 millones de dólares.

ción de un contrato de seguro que cubriese los daños generados al adherente, sin tener que demostrar nada más que el perjuicio económico.

La pérdida digital del activo y su posible reprogramación tiene una incidencia directa en la extinción de las obligaciones por destrucción de la cosa, de conformidad con el art. 1156 CC, así como en el uso de activos digitales como garantía real, en la línea de los *ELI Principles on the Use of Digital Assets as Security*[22], del European Law Institute, en adelante *ELI Principles*. La existencia de los activos digitales patrimoniales necesita la preservación de la *blockchain* en la que se almacenan sus metadatos, está condicionada a que no se produzca su desprogramación, y no le afecta la transmisión de carteras de activos digitales entre plataformas -incluyendo la sucesión de empresa- o su interoperabilidad, comprendiendo las *crypto wallets,* porque permanece su programación. En este sentido, presenta poca utilidad una propiedad digital que no sea interoperable, y ello requiere un diseño armonizado de la interfaz gráfica del usuario o GUI en las distintas plataformas en línea, siguiendo las obligaciones de accesibilidad de la DSA. Del mismo modo y en la línea de los *ELI Principles,* si se ha constituido una garantía real sobre un activo digital, solamente cabrá extinguirla por el cumplimiento de la obligación principal, además de por su desprogramación. En caso de desprogramación, se eliminan estos activos digitales de la plataforma, pero su constancia previa quedará registrada por la inmutabilidad del registro distribuido; en el entorno *off-chain,* en caso de pérdida o destrucción de un bien, será necesaria su cancelación registral. En atención a lo expuesto, no será posible calificar de pérdida del activo digital el olvido de las claves de acceso, pues la plataforma tendrá alojados los datos y, mediante los procedimientos que establezca, será posible recuperar las claves de acceso; tras la sucesión, debería establecerse la obligación al proveedor de la plataforma de facilitar a los herederos el acceso a la cuenta privada del causante y sus claves, si no se contienen expresamente en el testamento.

Por lo que respecta a la responsabilidad contractual establecida en la regulación europea sobre plataformas en línea -referida a la DSA, la DMA, y la *P2B Regulation*- el responsable civil será el usuario profesional frente al titular de los activos digitales. Solo responderá el proveedor de servicios de la plataforma por infracción de las obligaciones de diligencia debida o por haber realizado prácticas anticompetitivas -ateniéndose al régimen administrativo sancionador dispuesto para estas cuestiones respectivamente en la DSA y la DMA[23]-, así como cuando haya efectuado una actividad de intermediación y

---

[22] EUROPEAN LAW INSTITUTE (2022). *ELI Principles on the Use of Digital Assets as Security,* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf.

[23] WIELSCH, D. (2019). Private Law Regulation of Digital Intermediaries. *European Review of Private Law,* 27(2), 197-220. TERESZKIEWICZ, P. (2018). Digital Platforms: Regulation and

no concurra en las causas de exoneración de responsabilidad, dispuestas en los arts. 4-6 DSA en atención a la falta de relación de causalidad. Precisamos que, en atención al referido art. 6 DSA y en cumplimiento del art. 4 *P2B Regulation,* el proveedor de servicios de la plataforma también se exonera de responsabilidad por la suspensión o terminación del servicio de un usuario profesional, en el supuesto de afectación a los derechos de terceros, como en el referido caso de los *Metabirkins*.

Este régimen de responsabilidad civil contractual de las plataformas en línea es insuficiente, al menos, en los siguientes casos: por desprogramación de un activo digital -por un "hackeo" o por la vulneración de los derechos de terceros-, por colusión algorítmica -como práctica anticompetitiva parcialmente regulada en la *P2B Regulation* y la DMA-, y por discriminación algorítmica, carente de tratamiento legal específico. Por ello, a los efectos de evitar que el usuario profesional no responda como debe ante el consumidor y titular del activo digital desprogramado, y teniendo en cuenta que la *P2B Regulation,* la DSA y la DMA se van a modificar, -como ya se indicaba durante la tramitación de estos dos últimos, ante la escasa aplicación práctica del primero-, sería conveniente reformular esta responsabilidad en términos de *strict liability* o *semi-strict liability,* como se contiene en el estudio para el Parlamento Europeo *Liability of Online Platforms* y en la línea de lo aludido por la doctrina europea[24], ante la insuficiencia de las obligaciones de diligencia debida y el régimen administrativo sancionador.

A modo de reflexión prospectiva, los retos que plantea el Metaverso a los consumidores de activos digitales afectan principalmente a la protección de datos de carácter personal, referidos al control de identidad y los ficheros de

---

Liability in the EU Law. *European Review of Private Law,* 26(6), 903-920. RODRÍGUEZ DE LAS HERAS BALLELL, T. (2014). Refusal to Deal, Abuse of Right and Competition Law in Electronic Markets and Digital Communities. *European Review of Private Law,* 22(5), 685-702. MONTERO PASCUAL, J. J. (2024). *El reglamento de mercados digitales. La regulación de las grandes plataformas,* Valencia, Tirant lo Blanch, 113-255. BUESO GUILLÉN, P. J. (2023). Aproximación a las novedades en el derecho de defensa de la competencia de la Unión Europea en el tratamiento del uso de Internet por el distribuidor autorizado en los sistemas de distribución selectiva. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales,* Barcelona, Atelier, 259-280. HERRERO SUÁREZ, C. (2023). Merger control in digital markets: don't trust the trusts. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales,* Barcelona, Atelier, 227-239.

[24] EUROPEAN PARLIAMENT (2021). *Liability of online platforms,* European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf. CAUFMANN, C., GOANTA, C. (2021). A New Order: The Digital Services Act and Consumer Protection, *European Journal of Risk Regulation,* 1(1), 1-17. BÜYÜKSAGIS, E. (2022). Extension of Strict Liability to E-Retailers. *Journal of European Tort Law,* 13(1), 64-86. FROSIO, G. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review,* 112, 19-46.

solvencia, así como a los controles que les asisten como consumidores, debiendo destacar el control de transparencia. Ante los nuevos escenarios que pueden derivarse de la implementación de las nuevas tecnologías en la contratación B2C en las plataformas en línea, el control de incorporación es el único de los controles que asisten al consumidor cuya regulación actual sería suficiente, porque su cumplimiento podría comprobarse en dos estadios: *ab initio*, con la incorporación de las Condiciones Generales de la Contratación y la aceptación expresa del consumidor, mediante el "*I agree button*", de los términos y condiciones de uso de la plataforma correspondiente; y, durante su formación, a través la tecnología *blockchain*, que permite el cruce automático de información entre distintas instituciones para comprobar si las Condiciones Generales han sido incorporadas al contrato de manera transparente, para permitir su perfección. El ajuste legal del control de contenido, referido a las condiciones generales, y el control de transparencia de las condiciones particulares del contrato, por su componente subjetivo, pasa necesariamente por la regulación del papel que la IA y los algoritmos tengan en el *machine learning* de la plataforma y en los términos y condiciones de uso de esta, para adaptar la protección del consumidor atendiendo a la transparencia material del contrato.

3.2. La incardinación del régimen jurídico de las plataformas en línea en la responsabilidad extracontractual por los daños causados en las plataformas del Metaverso

Finalmente, en materia de responsabilidad civil extracontractual por los daños causados en las plataformas en línea inmersivas -en particular, las que conforman el Metaverso-, debemos armonizar la responsabilidad contractual de las plataformas con el régimen jurídico de la responsabilidad civil extracontractual. En atención a lo expuesto, la responsabilidad civil extracontractual por los daños causados en estas plataformas debería seguir también el sistema de responsabilidad objetiva referido en el estudio, en este caso, por el riesgo de la actividad, fundamentándolo en las siguientes razones: la manifiesta insuficiencia de las obligaciones de diligencia debida para disciplinar al proveedor de servicios de la plataforma; la dificultad para identificar y localizar al agente del daño sin la colaboración de la plataforma; y que el daño se produce en una plataforma creada y mantenida por su proveedor, que debe ofrecer un entorno digital seguro al usuario.

Apostar en este entorno por la responsabilidad civil subjetiva o por hecho propio, *ex* art. 1902 CC, plantea dos problemas: la prueba de la relación de causalidad, también aplicable a este contexto, al que se añade la difícil iden-

tificación y localización efectiva del agente del daño sin el establecimiento de una obligación legal de colaboración del proveedor de servicios de la plataforma, que necesariamente pasa por las obligaciones de diligencia debida de la responsabilidad civil por hecho ajeno. Por el contrario, un sistema de responsabilidad objetiva garantiza la necesaria disciplina del proveedor de servicios de la plataforma, pudiendo moderar su alcance: con una responsabilidad *fault-based system* -según consta en el estudio-, por ejemplo, por desprogramación del activo digital, por discriminación algorítmica, así como por los daños de carácter material o físico; con un sistema de *semi-strict liability,* correspondiente con nuestro sistema de responsabilidad por hecho ajeno por incumplimiento del deber de diligencia, por ejemplo, respecto de la colaboración aludida, advirtiendo de la falta de coercibilidad por las causas de exoneración de los arts. 4-6 DSA; o bien una responsabilidad civil objetiva por riesgo de la actividad o *strict liability*, que implicaría la cobertura de la responsabilidad por todo daño causado en estas plataformas.

El inconveniente que plantea el establecimiento de un sistema de responsabilidad objetiva absoluta o pura es la asunción de los costes de su aseguramiento obligatorio, pudiendo ser sufragados por vía de publicidad en la plataforma o mediante el pago de unas *fees* a cargo del usuario, lo que puede suponer su disminución, salvo que pueda monetizar su actividad en la plataforma. El establecimiento de un sistema de responsabilidad objetiva puede conllevar que algunas plataformas dejen de operar en la Unión, pudiendo restringir la exigencia de esta responsabilidad a las grandes plataformas en línea y los guardianes de acceso, en consonancia con los deberes agravados para estas plataformas previstos en la DSA y la DMA, respectivamente.

4. REFLEXIONES PROSPECTIVAS SOBRE LA RESPONSABILIDAD CIVIL CONTRACTUAL Y EXTRACONTRACTUAL: EL INFORME ESPAÑOL PARA LA COMISIÓN EUROPEA EN MATERIA DE CONTRATACIÓN CON INTELIGENCIA ARTIFICIAL

En este apartado, se formulan unas observaciones prospectivas en materia de responsabilidad civil contractual y extracontractual en materia de contratación automatizada, contratación con inteligencia artificial y contratos algorítmicos -referidos al uso de asistentes digitales-, a la luz del informe nacional de España emitido en autoría individual para la Comisión Europea en el estudio *"Novel forms of contracting in the digital economy",* respecto de los contratos de consumo y entre empresarios. Con carácter previo, es necesario indicar que las vías para regular la IA apuntadas por diversos académicos europeos serían

las siguientes: la prohibición de las decisiones totalmente automáticas, del art. 22 RGPD; la inclusión de un *algorithmic impact assessment,* del art. 35 RGPD, para la evaluación obligatoria de los algoritmos que afecten a derechos y libertades individuales; la monitorización y auditoría de los algoritmos; una regulación con remedios privados frente a la responsabilidad civil; y una regulación pactada entre las autoridades y las plataformas.

Considerando la responsabilidad civil por el uso de un sistema de IA proporcionado por un tercero para la contratación[25], la responsabilidad contractual implica un acuerdo mediante una licencia o servicio *ex* art. 1107 CC, que incluye la responsabilidad civil del proveedor de la IA por los errores causados por la IA en la contratación, y la responsabilidad extracontractual concierne al proveedor de la IA integrada en un determinado sistema, según el art. 1902 CC.

Con respecto a la responsabilidad contractual por el uso de un sistema de IA en la contratación, tal y como recomiendan los Principios 2 y 6 del Informe Provisional del *European Law Institute "EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM*[26]*?",* se debe proteger al consumidor por el uso de un asistente digital, considerando también la responsabilidad civil por falta de conformidad prevista en el art. 117 TRLGDCU. En este sentido, cabe mencionar que la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por productos defectuosos[27] protegerá a las personas físicas, incluidos los consumidores según los arts. 135 y 137 TRLGDCU, por los daños físicos y materiales causados por un sistema de IA, independientemente de si se proporciona dicho sistema en virtud de un contrato.

El tratamiento legal de la responsabilidad extracontractual de la IA integrada en un determinado sistema debe remitirse a la responsabilidad civil subjetiva o por hecho propio del art. 1902 CC, al no estar regulada en el ámbito de la responsabilidad por hecho ajeno prevista en los arts. 1903-1910 CC, ni en

---

[25] MARTÍN CASALS, M. (2023). Las Propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret,* 3, 55-100, https://indret.com/wp-content/uploads/2023/07/1806.pdf. YZQUIERDO TOLSADA, M. (2001). *Sistema de responsabilidad contractual y extracontractual,* Madrid, Dykinson, 1-545. PANTALEÓN PRIETO, F. (1991). El sistema de responsabilidad contractual. *Anuario de Derecho Civil,* 44(3), https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1991-30101901092, 1019-1092.

[26] EUROPEAN LAW INSTITUTE (2023). *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

[27] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por productos defectuosos, COM/2022/495 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A52022PC0495.

la legislación especial respecto de la responsabilidad objetiva. Por lo que respecta al requisito de la relación de la causalidad del art. 1902 CC, la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial[28] contiene una presunción *iuris tantum* de relación de causalidad en la responsabilidad civil subjetiva, prevista en el art. 4, de modo que el proveedor de un sistema de IA podría ser considerado responsable. En cuanto a la negligencia del contratante que utiliza la IA, la legislación española podría adaptarse para mantener la inversión de la carga de la prueba en el contexto de la responsabilidad subjetiva o por hecho propio, e incluso establecer un régimen de responsabilidad objetiva del proveedor de la IA.

BIBLIOGRAFÍA

ARGELICH COMELLES, C. (2022). El Derecho civil ante el Metaverso: hacia un Metalaw europeo y sus remedios en el Multiverso. *Derecho digital e innovación,* 12, 1-26.

ARRIETA SEVILLA, L. J. (2023). El uso de tokens en transmisiones inmobiliarias. *Revista de Derecho Civil,* X(2), 71-116.

ATZEI, N., BARTOLETTI, M., CIMOLI, T. (2017). A survey of attacks on Ethereum smart contracts. *Proceedings of the 6th International Conference on Principles of Security and Trust,* 10204, 1-23.

BUESO GUILLÉN, P. J. (2023). Aproximación a las novedades en el derecho de defensa de la competencia de la Unión Europea en el tratamiento del uso de Internet por el distribuidor autorizado en los sistemas de distribución selectiva. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales,* Barcelona, Atelier, 259-280.

BÜYÜKSAGIS, E. (2022). Extension of Strict Liability to E-Retailers. *Journal of European Tort Law,* 13(1), 64-86.

CAUFMANN, C., GOANTA, C. (2021). A New Order: The Digital Services Act and Consumer Protection, *European Journal of Risk Regulation,* 1(1), 1-17.

EUROPEAN LAW INSTITUTE (2019). *Model Rules on Online Platforms,* https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

[28] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, COM/2022/496 final, https://eur-lex.europa.eu/legal-content/EN /TXT/?uri=CELEX%3A52022PC0496.

EUROPEAN LAW INSTITUTE (2022). *ELI Principles on the Use of Digital Assets as Security,* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf.

EUROPEAN LAW INSTITUTE (2023). *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

EUROPEAN PARLIAMENT (2021). *Liability of online platforms,* European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf.

FETSYAK SENKIV, I. (2024). Impacto de la Propuesta de Reglamento de prevención de blanqueo de capitales en las transacciones con criptoactivos. ¿El fin de las «wallet» sin custodia y de las transacciones «crypto» anónimas?, *Diario La Ley,* 10487, 1-5.

FROSIO, G. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review,* 112, 19-46.

GARCÍA-TERUEL, R. M., SIMÓN-MORENO, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review,* 41, 1-16.

HERRERO SUÁREZ, C. (2023). Merger control in digital markets: don't trust the trusts. En GÓMEZ ASENSIO, C. (coord.), RUIZ PERIS, J. I., ESTEVAN DE QUESADA, C. (dirs.), *Cooperación y mercados digitales,* Barcelona, Atelier, 227-239.

KROLL, J., HUEY, J., BAROCAS, S., FELTEN, E., *et. al.* (2017). Accountable Algorithms. *University of Pennsylvania Law Review,* 165, 633-705, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

KRYSA, F. (2023). Taxonomy and Characterisation of Crypto Assets in Private International Law. En BONOMI, A., LEHMANN, M., LALANI, S., (eds.), *Blockchain and Private International Law,* Leiden, Brill, 157-208.

LACRUZ MANTECÓN, M. L. (2023). Propiedad Intelectual y tecnología inteligente. *Revista Crítica de Derecho Inmobiliario,* 99(800), 3103-3146.

MARTÍN CASALS, M. (2023). Las Propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret,* 3, 55-100, https://indret.com/wp-content/uploads/2023/07/1806.pdf.

MONTERO PASCUAL, J. J. (2024). *El reglamento de mercados digitales. La regulación de las grandes plataformas,* Valencia, Tirant lo Blanch.

NASARRE AZNAR, S. (2020). Naturaleza jurídica y régimen civil de los "tokens" en "blockchain". En GARCÍA TERUEL, R. M. (coord.), *La tokenización de bienes en blockchain: cuestiones civiles y tributarias,* Cizur Menor, Thomson Reuters Aranzadi, 61-108.

ORCUTT, M. (2019). Once hailed as unhackable, blockchains are now getting hacked. *MIT Technology Review,* https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

PACHECO JIMÉNEZ, M. N. (2022). De la digitalización de los pagos a los tokens del metaverso. *La Ley mercantil,* 91, 1-20.

PANTALEÓN PRIETO, F. (1991). El sistema de responsabilidad contractual. *Anuario de Derecho Civil,* 44(3), https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1991-30101901092, 1019-1092.

PARRONDO, L. (2023). Cryptoassets: Definitions and accounting treatment under the current International Financial Reporting Standards framework. *International Journal of Intelligent Systems in Accounting and Finance Management,* 4, 1-20.

RODRÍGUEZ DE LAS HERAS BALLELL, T. (2014). Refusal to Deal, Abuse of Right and Competition Law in Electronic Markets and Digital Communities. *European Review of Private Law,* 22(5), 685-702.

SCHULLER, R. R. (2022). Criptoactivos. Categorización jurídica de los criptoactivos e introducción a la tecnología DLT/Blockchain. *Cuadernos de Derecho Transnacional,* 14(2), 737-769.

TERESZKIEWICZ, P. (2018). Digital Platforms: Regulation and Liability in the EU Law. *European Review of Private Law,* 26(6), 903-920.

WALSHE, P. (2020). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention 108. Digital Identities. Council of Europe, 1-24, https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc-en/1680a0c051.%20/.

WHITTAKER, M., CRAWFORD, K., DOBBE, R., FRIED, G., *et. al.* (2018). *AI Now Report,* European Commission, Futurium, 1-63, ttps://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf.

WIELSCH, D. (2019). Private Law Regulation of Digital Intermediaries. *European Review of Private Law,* 27(2), 197-220.

YZQUIERDO TOLSADA, M. (2001). *Sistema de responsabilidad contractual y extracontractual,* Madrid, Dykinson.

La inteligencia artificial tiene el potencial de transformar productos, servicios y procedimientos en multitud de sectores económicos y en relación con muchos ámbitos de la sociedad. Sin embargo, también puede generar un sinfín de riesgos que, de producir daños, habrán de ser reparados. La Unión Europea no ha sido ajena a estos riesgos, y por ello ha pretendido y sigue pretendiendo crear un marco jurídico protector. Dentro de este contexto, se sitúa la aprobación del Reglamento (UE) 1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial -RIA-, como sendas Propuestas de Directiva, de inminente aprobación, sobre responsabilidad civil de productos defectuosos y sobre responsabilidad civil por daños causados por la inteligencia artificial. Partiendo de tales postulados, en la presente obra se han seleccionado aquellos sectores donde, por su mayor proyección, novedad o complejidad, merece ser analizada la interrelación entre la tecnología de la inteligencia artificial y el Derecho de daños. Para ello, se ha podido contar con un elenco de especialistas en el sector, que sin duda hace de la obra resultante una aportación doctrinal de indudable utilidad.

Con carácter particular, entre los sectores seleccionados, destaca por su trascendencia, el de la salud digital, donde problemáticas relacionadas con sistemas inteligentes para la prevención de enfermedades, ya sea a iniciativa del profesional de la medicina, o al margen de él -uso de werables y servicios digitales-, o por infracciones de los datos personales de salud, pueden determinar, si bien a través de distintos cauces normativos, posibles vías de reclamación indemnizatoria.

En el campo quirúrgico, la "cirugía 4.0", que integra la cirugía robótica y personalizada, por su creciente implantación, ha merecido una especial consideración en la obra.

Se efectúan igualmente amplías consideraciones acerca de la transparencia y explicabilidad para prevenir la discriminación algorítmica en el uso de los sistemas de inteligencia artificial.

Dentro de los sectores con mayor implementación de las tecnologías de inteligencia ha sido objeto de consideración así mismo el uso de vehículos autónomos, incluida su problemática en la vertiente del Derecho internacional privado.

Situados en el marco normativo que proporciona el Reglamento de Inteligencia artificial -RIA- se efectúan correspondientes análisis acerca de la categorización del riesgo que el mismo contempla, y donde se observa un régimen jurídico tendente a salvaguardar los riesgos más graves por el empleo de los sistemas de inteligencia artificial; en particular, en la salud, seguridad y derechos consagrados en la Carta Europea de Derechos Fundamentales. De igual forma las implicaciones jurídicas que despliega la inteligencia artificial generativa por infracciones normativas del Derecho de protección de datos personales. Se incluyen también los rasgos que deben estar presentes en el seguro de responsabilidad civil profesional de los operadores de inteligencia artificial, a partir de las previsiones normativas del referido Reglamento de Inteligencia Artificial.

9 788410 707085