ESTUDIOS

Incluye

HACIA UNA TRANSICIÓN DIGITAL CENTRADA EN LA PERSONA: ESTUDIOS JURÍDICOS DESDE LA PERSPECTIVA DE LA UNIÓN EUROPEA

JOSÉ JUAN CASTELLÓ PASTOR
COORDINADOR

ISABEL ANTÓN JUÁREZ
JOSÉ JUAN CASTELLÓ PASTOR
JOSÉ CORBERÁ MARTÍNEZ
CLARA ISABEL CORDERO ÁLVAREZ
ENRIQUE FERNÁNDEZ MASIÁ
ANA GASCÓN MARCÉN
ROSA LAPIEDRA ALCAMÍ
PATRICIA LLOPIS NADAL
ANTONIO MERCHÁN MURILLO
GUILLERMO PALAO MORENO
ROSA PLA ALMENDROS
ISABEL REIG FABADO

ARANZADI

HACIA UNA TRANSICIÓN DIGITAL CENTRADA EN LA PERSONA: ESTUDIOS JURÍDICOS DESDE LA PERSPECTIVA DE LA UNIÓN EUROPEA

Coordinador
JOSÉ JUAN CASTELLÓ PASTOR
Prof. Titular de Derecho Internacional Privado
Universitat de València

Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea

Autores

Isabel Antón Juárez
José Juan Castelló Pastor
José Corberá Martínez
Clara I. Cordero Álvarez
Enrique Fernández Masiá
Ana Gascón Marcén
Rosa Lapiedra Alcamí
Patricia Llopis Nadal
Antonio Merchán Murillo
Guillermo Palao Moreno
Rosa Pla Almendros
Isabel Reig Fabado

ARANZADI

© **José Juan Castelló Pastor y otros**, 2025
© **ARANZADI LA LEY, S.A.U.**

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/publicaciones

Proyecto de investigación del Ministerio de Ciencia, Innovación y Universidades titulado «Hacia una transición digital centrada en la persona en la Unión Europea» TED 2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea «NextGenerationEU»/PRTR. I.P. José Juan Castelló Pastor.

Primera edición: Noviembre 2025

Depósito Legal: M-23887-2025
ISBN versión impresa con complemento electrónico: 978-84-1163-776-3
ISBN versión electrónica: 978-84-1163-775-6

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

© **ARANZADI LA LEY, S.A.U.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, ARANZADI LA LEY, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.
Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, **www.cedro.org**) si necesita fotocopiar o escanear algún fragmento de esta obra.
El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.
El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.
ARANZADI LA LEY no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.
ARANZADI LA LEY queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.
ARANZADI LA LEY se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.
Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **ARANZADI LA LEY, S.A.U.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Consejo Asesor Aranzadi LA LEY

D. Luis María Cazorla (Presidente)
Presidente de la Real Academia de Jurisprudencia y Legislación de España

D. Alberto Palomar (Secretario)
Magistrado de lo contencioso-administrativo (EV)

D. Ricardo Alonso
Catedrático de Derecho Administrativo y de la UE

D. Moisés Barrio
Letrado del Consejo de Estado

D. Jacobo Manuel Barja de Quiroga López
Presidente de la Sala de lo Militar del Tribunal Supremo

D. Alfredo Berges
Presidente de UNE

D.ª Sonia Calaza
Decana de la Facultad de Derecho de la UNED
Catedrática de Derecho procesal de la UNED

D.ª Concepción Campos
Experta en Gestión Pública y Presidenta de la Asociación de Mujeres en el Sector Público

D.ª Ana Belén Campuzano
Catedrática de Derecho mercantil de la Universidad CEU San Pablo

D. Adolfo Díaz Ambrona
Secretario General de la Cámara de Comercio de España

D. Antonio Fernández de Buján y Fernández
Académico de Número de las Reales Academias de Jurisprudencia y Legislación de España y de Galicia

D.ª Isabel Fernández Torres
Catedrática (Ac.) de Derecho Mercantil

D.ª Ana Fernández-Tresguerres
Notaria de Madrid

D. José Luis García Delgado
Catedrático de Economía Aplicada. Univ. Nebrija

D.ª Piedad García-Escudero
Letrada de las Cortes Generales

D. Rafael García Meiro
Consejero Delegado/CEO de AENOR

D. Isaac Merino Jara
Magistrado del Tribunal Supremo (Sala de lo Contencioso-Administrativo)

D.ª Encarnación Roca
Catedrática de Derecho Civil

D. Antonio V. Sempere Navarro
Magistrado del Tribunal Supremo

D.ª Rosario Silva
Abogada del Estado

D. Eduardo Torres-Dulce
Fiscal

Presentación

La presente obra colectiva surge de la necesidad de reflexionar sobre las múltiples dimensiones que adopta el Derecho en el contexto digital, abarcando desde la protección de los consumidores hasta el impacto de la inteligencia artificial en la gobernanza global. A lo largo de sus doce capítulos, la obra aborda cuestiones de plena actualidad, como la vulnerabilidad del consumidor en línea, la protección de menores en entornos digitales, la regulación de los patrones oscuros, los mecanismos alternativos de resolución de litigios y la obtención de pruebas electrónicas. También se analizan los complejos desafíos que plantean la sucesión de bienes digitales y la consideración de los datos como bienes transnacionales. Destaca, además, el desarrollo normativo impulsado desde la Unión Europea y su diálogo con el Derecho internacional, orientado a adaptar los marcos regulatorios a los retos de la digitalización. En especial, se examina el papel de la inteligencia artificial en sus múltiples dimensiones: responsabilidad, derechos digitales, desinformación y riesgos sistémicos.

En su conjunto, se ofrece una visión de los esfuerzos legislativos —principalmente desde la Unión Europea— orientados a promover una transición digital centrada en la persona que preserve las garantías y los valores democráticos. Estos estudios representan una aportación significativa al debate sobre la evolución del Derecho en el entorno digital.

Esta obra colectiva es fruto de las reflexiones alcanzadas en la segunda etapa del proyecto de investigación del Ministerio de Ciencia, Innovación y Universidades titulado "Hacia una transición digital centrada en la persona en la Unión Europea" TED 2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea "NextGenerationEU"/PRTR cuyos autores forman parte del equipo de investigación y de trabajo. A todos ellos —procedentes de las Universidades de València, Complutense de Madrid, Cádiz, Zaragoza, Carlos III de Madrid; Castilla-La Mancha y Politécnica de València— les agradezco enormemente su trabajo, esfuerzo,

compañerismo y buen hacer, tan necesarios para el impulso de cualquier actividad organizada en el marco del proyecto.

José Juan Castelló Pastor

En Oporto, a orillas del río Duero un día de verano de 2025

BLOQUE I

Capítulo 1

Vulnerabilidad de los consumidores y usuarios en el entorno digital*

José Juan Castelló Pastor
Prof. Titular de Derecho Internacional Privado
Universitat de València
ORCID: 0000-0002-7517-0296

SUMARIO: I. PLANTEAMIENTO INICIAL. 1. *Repensar el marco jurídico digital para hacer frente a los daños actuales a los usuarios digitales*. 2. *Usuarios digitales: ¿una tutela jurisdiccional reforzada?* II. *CORPUS* JURÍDICO DIGITAL: *UNDE VENIMUS ET QUO IMUS*. III. LA CUADRATURA DEL CÍRCULO EN MATERIA DIGITAL. 1. *Instrumentalización de la atención y manipulación como recursos económicos de las plataformas digitales*. 2. *Medidas diseñadas para mitigar las técnicas de manipulación y adicción de las plataformas digitales*. IV. EQUIDAD DIGITAL: PATERNALISMO DEL REGULADOR VS. SOBERANÍA DEL CONSUMIDOR. V. REFLEXIÓN FINAL. BIBLIOGRAFÍA.

I. PLANTEAMIENTO INICIAL

1. REPENSAR EL MARCO JURÍDICO DIGITAL PARA HACER FRENTE A LOS DAÑOS ACTUALES A LOS USUARIOS DIGITALES

El entorno digital plantea desafíos que difícilmente encuentran paralelo en el ámbito analógico, como el uso de tecnologías altamente sofisticadas

* Esta publicación es parte del Proyecto TED2021-129307A-I00, financiado por MICIU/AEI /10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, cuyo investigador principal es el autor. Estudio realizado durante la estancia de investigación en el Centro de Investigación Interdisciplinaria sobre la Justicia de la facultad de Derecho de la Universidad de Porto (Portugal).

por parte de operadores digitales, capaces de anticipar, condicionar o incluso modificar el comportamiento de los usuarios. A pesar de los avances regulatorios impulsados por la Unión Europea —orientados a reforzar la transparencia, la seguridad de los usuarios y una gobernanza de las tecnológicas más equitativa—, ciertos colectivos continúan expuestos a notables vulnerabilidades.

En este escenario de constante transformación, asistimos a una auténtica revolución digital que, si bien ha sido asimilada con sorprendente rapidez, viene acompañada de una paradójica pérdida de control: vivimos hiperconectados, pero sometidos a dinámicas comerciales que mercantilizan nuestra atención[1].

Los datos así lo muestran. En promedio, las personas pasan más de siete horas al día conectadas a internet. Asimismo, uno de cada cuatro menores de dieciocho años manifiesta un patrón de uso problemático o disfuncional de los teléfonos inteligentes, expresando sensaciones de inseguridad o dependencia ante la ausencia de estos dispositivos y se observa, paralelamente, un incremento en los problemas de salud mental entre los adolescentes[2]. A estos preocupantes indicadores se suma el hecho de que una amplia mayoría de los consumidores percibe que las empresas tecnológicas vulneran sus derechos digitales. En efecto, solo un cuarenta y tres por ciento declara sentirse plenamente en control de sus decisiones en línea, mientras que las prácticas comerciales desleales representan el principal daño a los derechos de los usuarios en el entorno digital[3].

Todo esto evidencia que el actual marco jurídico digital de la Unión Europea necesita una actualización, esta vez, orientada explícitamente a pro-

---

1. El término "economía de la atención" se refiere al conjunto de actividades económicas basadas en la atención de las personas, considerada como un recurso escaso y muy deseable que hay que captar y mantener. *Vid*., Documento de Trabajo de la Comisión *Fitness Check of EU consumer law on digital fairness*, Brusselas, 3.10.2024. SWD (2024) 230 final, pág. 20.
2. Véase la Resolución del Parlamento Europeo, de 12 de diciembre de 2023, sobre el diseño adictivo de los servicios en línea y la protección del consumidor en el mercado único de la Unión (2023/2043(INI)).
3. Así lo indica el barómetro del consumidor de 2023, que el 70 % de los consumidores están preocupados por la forma en que se utilizan y comparten sus datos personales. Según la encuesta a los consumidores en el marco de la prueba de aptitud, el 37 % de los encuestados tenía la impresión de que una empresa conocía sus debilidades y utilizaba este conocimiento con fines comerciales.Véase, igualmente el informe de BEUC, *Connected but unfairly treated. Consumer survey results on the fairness of the online environment* (2023).

teger la vulnerabilidad del usuario digital, ya que, en el contexto actual, los intereses económicos de las tecnológicas están poniendo al límite nuestros derechos fundamentales recogidos en la Carta de los Derechos Fundamentales de la Unión Europea.

Y vaya por delante que un modelo de autorregulación no constituye, a mi modo de ver, una respuesta adecuada a los desafíos actuales, en tanto que estos gigantes tecnológicos subordinan la salvaguarda de las libertades digitales de los usuarios a sus propios intereses, instrumentalizando nuestra atención y manipulación como recursos económicos. No obstante, tampoco resulta evidente que un enfoque excesivamente paternalista del regulador de la Unión constituya una alternativa plenamente satisfactoria, como se estudia en este trabajo.

En cualquier caso, la Comisión Europea ha reconocido que el marco jurídico vigente de la Unión no puede considerarse suficientemente eficaz para hacer frente a los perjuicios actuales y emergentes que afectan a los consumidores[4]. De hecho, la presidenta de la Comisión Europea, Úrsula von Der Leyden, en la Mission Letter enviada a Michael McGrath, Comisario Europeo para la Democracia, la Justicia y el Estado de Derecho al inicio del segundo mandato, mostró su preocupación y marcó unas líneas de trabajo: "[…] me gustaría que desarrollara un marco de política común actualizado y presentara la próxima Agenda del Consumidor 2025-2030, en particular analizando cómo proteger a los consumidores vulnerables y evaluando la necesidad de actualizar la legislación y garantizar su aplicación. Como parte de esto, también debería proponer un nuevo Plan de Acción sobre los consumidores en el Mercado Único para garantizar que los consumidores no se enfrenten a una discriminación injusta, mantengan los beneficios al cruzar las fronteras y estén protegidos al comprar bienes y servicios. Me gustaría que se centrara en el impacto y las oportunidades de las tecnologías digitales

4. En concreto subraya que "[…] para lograr la equidad digital, el *Fitness Check* señala la necesidad de hacer más para abordar los retos pendientes en materia de protección de los consumidores en el entorno digital. Una lección clave aprendida es que un marco de protección de los consumidores sólido e independiente aporta un valor añadido a la hora de evaluar las prácticas comerciales en constante evolución en los mercados digitales. El marco jurídico vigente de la UE no puede considerarse suficientemente eficaz para hacer frente a los perjuicios actuales y emergentes que afectan a los consumidores. Si no se adoptan nuevas medidas, la legislación de la UE en materia de consumo no alcanzará plenamente sus objetivos, corre el riesgo de perder relevancia en el ámbito digital y puede seguir aplicándose solo en casos limitados" (traducción del autor). Véase el Documento de Trabajo de la Comisión *Fitness Check of EU consumer law on digital fairness*, Brusselas, 3.10.2024. SWD (2024) 230 final, pág. 88.

en los consumidores y nuestro sistema de justicia. Desarrollará una Ley de Equidad Digital para abordar las técnicas y prácticas comerciales poco éticas relacionadas con los patrones oscuros, el marketing de los *influencers* de las redes sociales, el diseño adictivo de productos digitales y la elaboración de perfiles en línea, especialmente cuando se explotan las vulnerabilidades de los consumidores con fines comerciales. Contribuirá a abordar los desafíos de las plataformas de comercio electrónico, en particular para proteger a los consumidores y garantizar que se beneficien de una igualdad de condiciones. También impulsará nuestros esfuerzos para modernizar, implementar y hacer cumplir las políticas de seguridad de los productos. Garantizará que la Unión Europea siga siendo un referente mundial en materia de protección del consumidor y seguridad de los productos[5]".

2. USUARIOS DIGITALES: ¿UNA TUTELA JURISDICCIONAL REFORZADA?

Uno de los aspectos más significativos, a mi modo de ver, viene referido al término usuario digital como sujeto vulnerable *per se* en este entorno tecnológico. A este respecto, la política digital de la Unión Europea parece estar dando prioridad a configurar categorías genéricas —con términos más inclusivos— que engloban el papel que desempeñan las personas en estos nuevos entornos tecnológicos[6].

Sirva a modo de ejemplo el Reglamento (UE) 2022/2065 de servicios digitales, que si bien define al consumidor como toda persona física que actúe con fines ajenos a su actividad comercial, negocio, oficio o profesión[7], también se introducen, no obstante, otras categorías adicionales que van difuminando a esta figura, como la del destinatario del servicio, entendida como toda persona física o jurídica que utilice un servicio intermediario, en particular para buscar información o para hacerla accesible[8], y la del destinatario activo (de una plataforma o de un buscador) que es el destinatario del servicio que haya utilizado una plataforma en línea, bien solicitando a la plataforma que aloje información, bien exponiéndose a la información

5. Disponible en la página commission.europa.eu.
6. NAMYSŁOWSKA, M.: "The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices", *Journal of Consumer Policy*, 2025 (versión en línea).
7. En las definiciones incorporadas en el artículo 3 letra c) del Reglamento (UE) de servicios digitales.
8. De acuerdo con la definición del artículo 3 letra b) del Reglamento (UE) de servicios digitales.

alojada en la plataforma en línea y difundida a través de su interfaz en línea[9]. Además, este mismo texto normativo se refiere al usuario en el artículo 25 en relación con el diseño y organización de interfaces en línea, a la amplia categoría de ciudadanos en el artículo 45.3 sobre los códigos de conducta y a la de destinatarios como se ha referido.

De este modo, como se observa, coexisten el consumidor, el destinatario del servicio y otras categorías genéricas. Y no solo en este texto jurídico-digital, sino también en otras normativas tecnológicas como por ejemplo en el Reglamento (UE) 2022/1925 de mercados digitales o más recientemente en el Reglamento (UE) 2024/1689 de inteligencia artificial. Así cabe referirse al término usuarios finales en el artículo 20.2 del Reglamento (UE) 2022/1925 de mercados digitales y en el artículo 71 del Reglamento (UE) 2024/1689 de inteligencia artificial y a la categoría de personas físicas utilizada en el artículo 78 del Reglamento (UE) 2024/1689 de Inteligencia Artificial.

Por este motivo cabe preguntarse si resulta oportuno reforzar la protección del usuario digital mediante una tutela jurisdiccional especial. Dicho de otro modo, si en el marco normativo de la competencia judicial internacional sería oportuno establecer una regla específica en materia digital —una idea que está presente en las infracciones a los derechos de la personalidad cometidas en la red por parte de la doctrina[10]—.

---

9. De acuerdo con la definición del artículo 3 letra p) del Reglamento (UE) de servicios digitales.

10. Véase HESS, B.: "Reforming the Brussels Ibis Regulation: Perspectives and Prospects", *MPILux Research Paper Series*, 4, 10, 2021 y, como subrayé en otro estudio, véase CASTELLÓ PASTOR, JJ.: "Por un foro de competencia judicial internacional para favorecer al vulnerable de los comportamientos lesivos a los derechos de la personalidad en internet" en *Protección multidisciplinar del vulnerable en la sociedad digital* (Coord. BLANCO GARCÍA. A.I.), Aranzadi, 2024, págs. 75-76: "[…] es cierto que la jurisprudencia del Tribunal de Justicia de la Unión Europea ha creado un foro digital en la que la víctima puede reclamar la totalidad de los daños ante los tribunales de su residencia habitual —condicionado a que coincida con su centro de intereses—. Se trata de meritoria regla tuitiva que mitiga la vulnerabilidad del usuario frente a los exponenciales efectos de cualquier publicación en internet. Sin embargo, desde mi punto de vista, sería deseable que —en una revisión del Reglamento Bruselas I bis— se incorpore una regla especial de competencia judicial internacional para estos ilícitos cibernéticos de forma que la víctima no tuviera que probar su centro de intereses para interponer la acción civil por la totalidad de los daños causados por una publicación digital ante los tribunales del Estado miembro de su domicilio. Esta nueva regla especial y tuitiva de competencia judicial internacional podría ser aplicable a todas las personas físicas y jurídicas —estas últimas sólo para las microempresas o pequeñas empresas definidas en la Recomendación 2003/361/CE para evitar cargas desproporcionadas al disponer de recursos limitados—, de modo que podría recurrirse a este *forum actoris* digital

A mi parecer, la respuesta debe ser afirmativa, encontrándose el punto de partida de esta nueva regla especial y tuitiva de competencia judicial internacional en el concepto de vulnerabilidad aplicado a los usuarios como consumidores, que, en este contexto tecno-digital, debería ampliarse para incluir también a los ciudadanos en general. Esta nueva regla tuitiva en favor del usuario —en términos generales— como vulnerable digital facilitaría esencialmente la determinación del tribunal competente en caso de verse afectado, por ejemplo, por un riesgo sistémico; en consonancia con la idea de que la transición digital debe estar centrada en la persona.

Sentado lo anterior, el presente estudio se centra en uno de los temas más trascendentes en el ámbito de los derechos de los consumidores y usuarios digitales: los efectos perjudiciales que generan las plataformas —ya sean de comercio electrónico, redes sociales u otras— mediante el uso de técnicas deliberadamente diseñadas para influir en la conducta y captar su atención. En este sentido, el trabajo se estructura en tres partes: en primer término, se presenta un examen sintético del marco jurídico digital actualmente vigente; en segundo lugar, se analiza el modo en el que las tecnológicas orientan y condicionan la atención de los usuarios, así como las respuestas regulatorias adoptadas para contrarrestar estas prácticas; finalmente, se ofrece una reflexión crítica sobre la regulación futura en materia de equidad digital, subrayando que una posible sobrerregulación del legislador de la Unión —motivada por un enfoque excesivamente paternalista o por una tendencia a reforzar su tutela— pudiera, en determinadas circunstancias, limitar el ámbito de su autonomía y responsabilidad individual del usuario digital, con el consiguiente menoscabo de su capacidad en la toma de decisiones.

II. *CORPUS* JURÍDICO DIGITAL: *UNDE VENIMUS ET QUO IMUS*

Resulta complejo prever cómo será la sociedad en la próxima década, dada la profundidad y rapidez de los cambios que las innovaciones tecnológicas han generado —y continúan generando— en la sociedad[11]. Una de las preocupaciones del legislador de la Unión es cómo afrontar de manera

---

aunque el contenido lesivo publicado en internet no tuviera impacto real en el Estado miembro de la residencia habitual de la víctima, pero sí en otros Estados miembros, y permitirle de este modo reclamar la totalidad del daño sufrido por la publicación".

11. En este sentido, la inteligencia artificial se perfila como un elemento disruptivo de gran relevancia, con el potencial de transformar significativamente la sociedad tal como la conocemos. Al igual que hizo —y continúa haciendo— internet, la inteligencia artificial se proyecta como una tecnología transversal capaz de incidir en múltiples dimensiones de la vida cotidiana.

eficaz el impacto de las tecnologías emergentes en la sociedad contemporánea. Desde la irrupción de internet en la década de 1990, hemos sido testigos de una transformación socioeconómica sin precedentes[12].

La digitalización ha dado lugar a una economía global interconectada, que funciona a una velocidad y escala inimaginables hace apenas unas décadas. La adopción generalizada de internet facilitó el surgimiento de los primeros modelos de negocio digitales que comenzaron a consolidarse en los primeros años del presente siglo[13]. Este desarrollo no habría sido posible sin un entorno regulatorio favorable que, durante las últimas décadas, ha permitido el crecimiento exponencial y el fortalecimiento del ecosistema tecnológico en la Unión. En este escenario, la labor normativa de las instituciones de la Unión Europea se ha orientado a capacitar a empresas y ciudadanos, con la finalidad de configurar un futuro digital centrado en las personas, sostenible y próspero.

Ya en el marco de la Estrategia de Lisboa, la (primera) Agenda Digital para Europa[14] del año 2010 reconocía el papel estratégico de las tecnologías de la información y la comunicación en el logro de los objetivos de desarrollo e integración de la Unión. Posteriormente, en el año 2015, la Estrategia para el Mercado Único Digital[15] propuso medidas para mejorar el acceso a bienes y servicios digitales en toda la Unión, establecer condiciones óptimas para el despliegue de redes y servicios digitales, y ampliar el potencial de crecimiento de la economía digital. En el año 2020, la Unión avanzó hacia la configuración de su futuro digital mediante una estrategia orientada a

12. Es opinión generalizada que la revolución tecnológica de estas últimas décadas ha generado un impacto social y económico sin precedentes en la historia de nuestra civilización desde la expansión del uso de internet a principios de la década de 1990. Este fenómeno representa un auténtico cambio de era que supera en efecto y significado a la primera revolución industrial del siglo XVIII e incluso a la Revolución Francesa de 1789. *Vid*. BARRIO ANDRÉS, M.: "Inteligencia artificial, Internet de las cosas y blockchain", en MONTERO PASCUAL, J.J., *Digitalización y Derecho*, Tirant Lo Blanch, Valencia, 2024, pág. 253.
13. La accesibilidad a la red facilitada por la proliferación de dispositivos inteligentes, junto con la disponibilidad de conexiones a través de fibra y redes inalámbricas con tarifas muy asequibles, entre otros factores, fomentó la fidelización de los usuarios hacia el consumo de contenidos y servicios digitales. Asimismo, la significativa inversión de la industria tecnológica contribuye a consolidar este hábito digital de los usuarios europeos, desplazando progresivamente a su homólogo tradicional. Esta distancia entre lo analógico y digital se amplía aún más con la tecnología 5G y la inteligencia artificial, transformando la interacción y el consumo digitales, e incluso conduciendo a una sociedad excesivamente dependiente de la tecnología, como se ha referido.
14. Bruselas, 19.5.2010. COM (2010) 245 final.
15. Bruselas, 6.5.2015. COM (2015) 192 final.

situar la tecnología al servicio de las personas, promover una economía más competitiva y reforzar una sociedad abierta y democrática[16]. Finalmente, en el año 2021, la iniciativa Brújula Digital[17] definió los objetivos estratégicos de la Unión en materia digital para 2030, organizados en torno a cuatro ejes fundamentales: desarrollo de capacidades digitales, refuerzo de la gobernanza, transformación de las empresas e inversión en infraestructuras digitales.

Efectivamente, desde la década de los noventa, la Unión Europea ha venido adoptando un conjunto progresivo de medidas legislativas orientadas a abordar los desafíos del entorno digital, así como a garantizar su efectiva implementación[18]. Muchas de estas normativas han sido objeto de procesos de modernización y europeización[19] en los últimos años, en respuesta a la acelerada evolución tecnológica y al crecimiento exponencial del ecosistema digital.

En este contexto, la Estrategia Europa 2020 —diseñada con el propósito de convertir la economía europea en la más competitiva y sostenible del mundo[20]— incorporó como una de sus siete iniciativas emblemáticas la

16. Bruselas, 19.2.2020. COM (2020) 67 final.
17. Bruselas, 9.3.2021. COM (2021) 118 final.
18. Entre otras, sirva a modo de ejemplo la Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador; la Directiva 92/100/CEE del Consejo, de 19 de noviembre de 1992, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual; la Directiva 93/83/CEE del Consejo, de 27 de septiembre de 1993, sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable; Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia; Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónico. Y a principios de la siguiente década, como la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior o la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
19. Léase el comunicado de prensa de la Comisión Europea de 6 de mayo de 2015 titulado "Un mercado único digital para Europa: la Comisión establece 16 iniciativas".
20. Fue uno de los objetivos de la Estrategia de Lisboa, literalmente señala que "la Unión se ha fijado hoy un nuevo objetivo estratégico para la próxima década: convertirse en la economía basada en el conocimiento más competitiva y dinámica del mundo,

Agenda Digital para Europa. Esta primera hoja de ruta digital, impulsada bajo el mandato del entonces presidente de la Comisión Europea, José Manuel Durão Barroso (2004-2014), tenía como objetivo principal acelerar el despliegue de redes de internet de alta velocidad y maximizar los beneficios del mercado único digital para ciudadanos y empresas en toda la Unión[21]. En consonancia con esta visión estratégica, su sucesor, Jean-Claude Juncker (2014-2019), subrayó en su discurso inaugural ante el Parlamento Europeo la necesidad de aprovechar plenamente el potencial de las tecnologías digitales, caracterizadas por su naturaleza transfronteriza. En sus propias palabras, abogó por "tener el valor de abrir los compartimentos nacionales de regulación de las telecomunicaciones, de los derechos de propiedad intelectual y de la legislación sobre protección de datos, de la gestión de las ondas de radio y de la aplicación del derecho de la competencia", con el fin de garantizar que "los consumidores puedan acceder a los servicios, la música, las películas y los eventos deportivos con sus dispositivos electrónicos en cualquier punto de Europa e independientemente de fronteras"[22]. En aquel momento, las proyecciones económicas estimaban que la concreción de una Unión digital plenamente funcional podría contribuir con aproximadamente cuatrocientos mil millones de euros anuales, así como generar cientos de miles de nuevos empleos en sectores estratégicos[23]. A la luz de estas perspectivas y sobre la base de los marcos estratégicos previamente establecidos, la Comisión Europea emprendió una ambiciosa labor legislativa, que daría forma al núcleo normativo del Mercado Único Digital, consolidando así una de las apuestas más trascendentales de la integración europea en el siglo XXI.

Esta (primera) Agenda Digital para Europa (2010-2020), concebida como una de las siete iniciativas emblemáticas de la Estrategia Europa 2020, permitió la consecución de diversos hitos clave en el ámbito del desarrollo tecnológico y la consolidación del mercado único digital. Sin ánimo de exhaustividad, pueden destacarse los siguientes logros normativos que contribuyeron significativamente a la transformación digital del espacio europeo: la mejora del acceso y reducción de costes en las comunicaciones electrónicas. Uno de los avances más relevantes en este sentido fue la eliminación de los recargos

---

capaz de crecer económicamente de manera sostenible con más y mejores empleos y con mayor cohesión social". *Vid*., Consejo Europeo de Lisboa, 23 y 24 de marzo 2000, Conclusiones de la Presidencia, punto I.5.

21. Bruselas, 3.3.2010. COM (2010) 2020 final.
22. Bruselas, 6.5.2015. COM (2015) 192 final.
23. De acuerdo con la información facilitada en la web de la Comisión Europea en aquel momento, si bien es cierto que algunos informes apuntaban a números superiores, como el Informe de 21 de diciembre de 2015 sobre la iniciativa "Hacia un mercado único digital" (2015/2147(INI).

por itinerancia dentro de la Unión Europea, efectuada el 14 de junio de 2017, en virtud del Reglamento (UE) 2022/612, que regula la itinerancia en redes públicas de comunicaciones móviles. Esta medida supuso una democratización efectiva del acceso transfronterizo a los servicios móviles, impulsando la cohesión digital en el espacio europeo. También, la ampliación de la conectividad digital: se garantizó la cobertura universal de banda ancha básica, mediante el aprovechamiento de tecnologías móviles y satelitales, lo que permitió cerrar brechas territoriales en el acceso a internet, en línea con los objetivos de inclusión digital de la Unión.

Por su parte, el refuerzo de la protección de los consumidores en el entorno digital: se adoptaron marcos clave en materia de privacidad y protección de datos, entre los que destacan la Directiva 2009/136/CE de 25 de noviembre de 2009 y el Reglamento (UE) 2016/679 del 27 de abril de 2016 y la Directiva (UE) 2016/680 del 27 de abril de 2016). Asimismo, la eliminación de barreras en el comercio digital transfronterizo: para fortalecer la libre circulación de servicios digitales, se adoptaron dos significativas normas como el Reglamento (UE) 2018/302 del 28 de febrero de 2018 sobre bloqueo geográfico injustificado y el Reglamento (UE) 2017/1128 del 14 de junio de 2017 sobre portabilidad transfronteriza de servicios digitales permitiendo a los consumidores acceder a contenidos en línea en toda la Unión Europea. En relación con la regulación de las relaciones contractuales digitales: se armonizaron las normas sobre contratos de compraventa de bienes y contratos de suministro de contenidos digitales mediante la Directiva (UE) 2019/770 y la Directiva (UE) 2019/771. En materia de transparencia en plataformas digitales: el Reglamento (UE) 2019/1150 introdujo medidas para fomentar la equidad y la transparencia en las relaciones entre las plataformas digitales y sus usuarios profesionales, consolidando una gobernanza más equilibrada del ecosistema de intermediación en línea. Y por último se centró en el fomento de una economía basada en los datos: con la visión de facilitar un entorno ágil y competitivo en el ámbito del tratamiento de datos no personales, la Unión Europea aprobó un conjunto de normas específicas, entre las que destacan: el Reglamento (UE) 2018/1807, que garantiza la libre circulación de datos no personales, permitiendo a las empresas y administraciones almacenar y procesar información en cualquier Estado miembro; el Reglamento (UE) 2019/881, relativo a la ciberseguridad, que establece un marco europeo de certificación en la materia y la Directiva (UE) 2019/1024, relativa a los datos abiertos y la reutilización de la información del sector público, con el objetivo de promover la innovación y el uso estratégico de los datos en beneficio del interés general.

En aquel entonces, se abordó, a mi modo de ver, uno de los desafíos más significativos del entorno digital: la necesidad de reducir las asimetrías existentes entre el ámbito digital y el analógico en el contexto de las actividades transnacionales en línea[24]. En efecto, la Comisión Europea adoptó un firme compromiso con la eliminación de los obstáculos que impedían la plena realización del mercado único digital, concebido como un proyecto esencial dentro de una Unión caracterizada por la supresión de fronteras físicas y por la vigencia de las cuatro libertades fundamentales. La segmentación de los mercados en función de las fronteras nacionales, habitualmente sin justificación objetiva, resultaba incompatible con los principios que rigen el Tratado de Funcionamiento de la Unión Europea. En este sentido, el desarrollo del mercado único digital, estrechamente vinculado con el concepto de mercado interior[25], se definió como un espacio en el que se garantiza la libre circulación de mercancías, personas, servicios y capitales, y en el que ciudadanos y empresas pueden acceder y participar en actividades económicas en línea en condiciones de competencia equitativa, con un alto nivel de protección de los datos personales y de los derechos de los consumidores, independientemente de su nacionalidad o lugar de residencia[26].

Una vez alcanzado con éxito el objetivo estratégico del mercado único digital[27], la nueva Comisión Europea, presidida por Ursula von der Leyen (2019-2024), dio continuidad a las líneas de acción establecidas por su pre-

24. Eliminando cualquier traba o discriminación existente ya que se daban prácticas comerciales que difícilmente encontraban apoyo —salvo en contadas excepciones— en uno de los objetivos generales de la Unión Europea, a saber: el establecimiento del mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones de los Tratados. Así se pronunció en su momento la STJ de 11 de julio de 1974, as. 8/74, *Dassonville*, (EU:C:1974:82), apdo. 5, señalando que "[…] toda normativa comercial de los Estados miembros que pueda obstaculizar directa o indirectamente, real o potencialmente, el comercio intracomunitario debe considerarse como una medida de efecto equivalente a las restricciones cuantitativas".
25. Art. 26.2 del TFUE.
26. Bruselas, 6.5.2015, COM (2015) 192 final. En síntesis, la Estrategia para el mercado único digital consiste en mejorar el acceso de los consumidores y las empresas a los bienes y servicios en línea; crear condiciones adecuadas y equitativas para el éxito de las redes digitales y los servicios innovadores; y aprovechar al máximo el potencial crecimiento de la economía digital.
27. Aunque la rápida transformación digital unido al incremento de las transacciones en línea en estos últimos años ponen de manifiesto la importancia de reevaluar la normativa relacionada con el bloqueo geográfico para eliminar las barreras restantes y maximizar, así, el potencial del mercado único de la Unión conforme subrayó un grupo de diputados al Parlamento Europeo el 13 de diciembre de 2023.

decesor, al tiempo que introdujo una renovada visión política a través de la definición de seis prioridades estratégicas para su mandato. Entre ellas destacó la construcción de una Europa adaptada a la era digital[28], orientada a situar la tecnología al servicio de las personas, fomentar una economía digital justa y competitiva, y promover una sociedad abierta, democrática y sostenible[29].

Esta (segunda) Agenda Digital para Europa (2020-2030) se centró en gestionar los profundos cambios inducidos por las tecnologías digitales y en resaltar la importancia estratégica de los servicios y mercados digitales. En efecto, esta nueva fase se caracterizó por una clara dimensión tecnológica y geopolítica, mediante la cual la Unión Europea buscó afirmar su autonomía y liderazgo en la esfera digital global. Una prioridad posteriormente desarrollada en documentos clave como la comunicación "Configurar el futuro digital de Europa[30]" y la comunicación sobre la "Década Digital de Europa", donde se trazaron las líneas de actuación para asegurar la seguridad de los servicios y mercados digitales. Asimismo, se otorgó prioridad a áreas tecnológicas de alto impacto como las estrategias en blockchain, el desarrollo ético y responsable de la inteligencia artificial, el diseño y producción de semiconductores avanzados, la consolidación de la soberanía digital europea, y la creación de espacios europeos de datos, así como a la promoción de normas tecnológicas globales acordes con los valores de la Unión, entre otras medidas.

Esta prioridad estratégica en el ámbito digital durante el último lustro se ha traducido en una intensa y prolífica actividad legislativa por parte de las instituciones de la Unión Europea, dando lugar a un *corpus* normativo de gran relevancia jurídica y política en el marco del proceso de digitalización.

Entre las principales normativas adoptadas destacan: el Reglamento (UE) 2022/2065 de servicios digitales, cuyo objetivo es actualizar las reglas de los intermediarios, esencialmente por medio de la transparencia en la gobernanza de las plataformas y diligencia debida; el Reglamento (UE) 2022/1925, sobre mercados digitales, cuyo objetivo es limitar las prácticas anticompetitivas de los grandes operadores de plataformas consideradas "guardianes de acceso"; el Reglamento (UE) 2024/1689, sobre inteligencia artificial, que constituye el primer marco legal integral sobre el desarrollo,

28. Orientaciones políticas para la próxima Comisión Europea (2019-2024).
29. Léase el discurso ante la sesión plenaria del Parlamento europeo pronunciado por la presidenta electa de la Comisión Europea Ursula von der Leyen el 27 de noviembre de 2019.
30. Bruselas, 19.2.2020, COM (2020) 67 final.

la comercialización y el uso de sistemas de IA dentro del territorio de la Unión; el Reglamento (UE) 2021/784, centrado en la lucha contra la difusión de contenidos terroristas en línea, que impone obligaciones estrictas a los proveedores de servicios para la retirada rápida de dichos contenidos; el Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos, y el Reglamento (UE) 2023/2854, conocido como Reglamento de Datos, ambos destinados a fomentar la disponibilidad, el intercambio seguro y el acceso equitativo a los datos industriales, personales y públicos, entre otros.

A lo anterior cabe añadir que el Parlamento Europeo ha desempeñado también un papel activo por la adopción de diversas resoluciones estratégicas, especialmente en materia de inteligencia artificial. Cabe mencionar, al respecto, la resolución 2020/2012 (INL), sobre las implicaciones éticas de la IA; la resolución 2020/2014 (INL), relativa a la responsabilidad civil derivada del uso de sistemas de IA; la resolución 2020/2015 (INI), que aborda el impacto de la IA sobre los derechos de propiedad intelectual; así como la resolución 2023/2043 (INI), que impulsa la prohibición del uso de técnicas adictivas en el diseño de servicios digitales dirigidos a manipular el comportamiento del usuario. Igualmente, en línea con los valores democráticos de la Unión, se han adoptado otras normas emblemáticas como: el Reglamento (UE) 2024/1083, sobre la Libertad de los Medios de Comunicación, destinado a proteger la independencia editorial y prevenir injerencias indebidas en los medios y el Reglamento (UE) 2024/900, relativo a la transparencia y segmentación en la publicidad política, que busca garantizar elecciones más limpias y una comunicación política más justa y transparente en el entorno digital, entre otras.

El conjunto de estos actos jurídicos adoptados en los últimos años, junto con otras iniciativas normativas, pone de manifiesto la capacidad legislativa de las instituciones de la Unión Europea para definir un marco normativo propio en el contexto tecnológico. Este ejercicio normativo autónomo en el mundo digital constituye un paso decisivo en la construcción de nuestra soberanía digital[31], entendida no solo como la capacidad de innovación tecnológica, sino también como la potestad de regular conforme a principios y valores propios.

En este sentido, la Unión Europea no solo ha avanzado en la regulación de un sector tecnológico históricamente dominado por actores situados en terceros Estados —en particular, por gigantes tecnológicos estadouniden-

31. MADIEGA T.: "Digital sovereignty for Europe", *EPRS Ideas Paper Towards a more resilient EU*, 2020, pág. 1.

ses—, sino que, a mi modo de ver, logra algo más relevante: proyectar los valores fundamentales de la Unión a través de la extraterritorialidad normativa que deriva del acceso al mercado interior[32]. Así, el cumplimiento del marco jurídico digital de la Unión se ha convertido en una condición de acceso para cualquier operador económico que desee prestar servicios dentro de la Unión, lo que refuerza su posición como potencia regulatoria global en el ámbito digital[33].

Finalmente, el 18 de julio de 2024, Ursula von der Leyen, reelegida como presidenta de la Comisión Europea para un segundo mandato, presentó ante el Parlamento Europeo las directrices políticas que orientarán la acción de la Comisión Europea durante el período 2024-2029. En su intervención, delineó una hoja de ruta centrada en el fortalecimiento y la consolidación de la unidad europea, al tiempo que expuso las prioridades estratégicas de su nueva gestión. Entre los ejes prioritarios, y en lo que interesa al presente trabajo, subrayó la necesidad de estimular la productividad a través de la expansión de las tecnologías digitales, advirtiendo que la competitividad europea se ve limitada en comparación con la de sus principales competidores globales, debido en gran parte a una insuficiente adopción de instrumentos digitales. Esta carencia afecta negativamente la capacidad de la Unión para innovar en servicios y modelos de negocio.

Así, anunció que la nueva Comisión centrará sus esfuerzos en la implementación efectiva de la legislación digital adoptada durante el mandato anterior, haciendo especial énfasis en la responsabilidad que deben asumir las grandes plataformas tecnológicas, dadas las implicaciones sistémicas de su poder en las dinámicas sociales y económicas actuales. En este contexto, se reforzará la aplicación del Reglamento (UE) 2022/2065 de Servicios Digitales y el Reglamento (UE) 2022/1925 de Mercados Digitales, avanzando hacia un entorno digital más justo y equilibrado. Asimismo, se abordarán los desafíos derivados del crecimiento de las plataformas de comercio electrónico, con el objetivo de garantizar condiciones de competencia equitativas para consumidores y empresas, sustentadas en normativas eficaces en materia aduanera, fiscal, de seguridad y de sostenibilidad. La presidenta de la Comisión concluyó que el cumplimiento de los objetivos digitales y la consolidación de un verdadero mercado único digital podrían representar

32. CHRISTAKIS, T.: *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, 2020, pág. 2.

33. Este fenómeno, conocido como el "efecto Bruselas", ilustra cómo la Unión Europea, incluso actuando de forma unilateral, puede influir en los estándares globales, imponiendo *de facto* sus normas más allá de sus fronteras mediante el poder de atracción de su mercado.

un punto de inflexión crucial para mejorar tanto la productividad como la competitividad de Europa[34].

No obstante, persiste la incertidumbre sobre el futuro inmediato de esta agenda regulatoria, especialmente en el contexto de las tensiones transatlánticas. En particular, se ha planteado la posibilidad de que el *corpus* normativo digital europeo se convierta en objeto de negociación política con la nueva administración Trump, en el marco de eventuales discusiones comerciales y arancelarias. El Gobierno de Estados Unidos ha manifestado en múltiples ocasiones su oposición frontal a determinadas disposiciones del Reglamento (UE) 2022/2065 de servicios digitales, alegando que sus disposiciones podrían suponer una amenaza para la libertad de expresión y resultar discriminatorias para las empresas estadounidenses.

Queda por ver si, en un escenario de creciente fricción económica, la Comisión Europea mantendrá su postura regulatoria firme o se verá presionada a reconsiderar ciertos aspectos normativos como parte de una negociación geopolítica más amplia.

III. LA CUADRATURA DEL CÍRCULO EN MATERIA DIGITAL

Con una generación de nativos digitales, el acceso a internet se ha convertido un elemento esencial para la realización de prácticamente cualquier actividad a través de las aplicaciones, redes sociales y, en términos más amplios, plataformas digitales.

La expansión de estas herramientas digitales ha dado lugar a un entorno marcado por una oferta prácticamente ilimitada de contenidos y servicios, lo que ha contribuido al aumento del tiempo que los usuarios permanecen frente a las pantallas de sus dispositivos. Una tendencia que responde, en buena medida, a la habilidad de las tecnológicas para anticipar y satisfacer las necesidades de los usuarios, que conlleva también considerables efectos adversos —entre los que se destaca el impacto negativo sobre la salud mental por estar continuamente pendiente de la red[35]—.

La verdadera cuadratura del círculo en la regulación digital radica hoy en día en la capacidad de mitigar los efectos adversos provocados por las plataformas digitales —sean de comercio electrónico, redes sociales u otras—

34. Visítese la página web de la Comisión y las Orientaciones políticas 2024-2029.
35. Téngase presente este problema actual de la adicción digital y salud mental. Aunque no se aborda en este trabajo, será objeto de un futuro estudio los menores en el entorno digital.

cuyo diseño deliberado busca manipular y mantener la atención constante del usuario.

Tal como se ha expuesto en el planteamiento inicial, el marco jurídico vigente de la Unión Europea muestra importantes limitaciones para afrontar, con eficacia, los daños actuales y potenciales que sufren los consumidores.

Este escenario plantea la necesidad de repensar y posiblemente adaptar el marco legal para ofrecer una protección más acorde con los desafíos que plantea la evolución tecnológica.

1. INSTRUMENTALIZACIÓN DE LA ATENCIÓN Y MANIPULACIÓN COMO RECURSOS ECONÓMICOS DE LAS PLATAFORMAS DIGITALES

Mas allá de los mencionados objetivos políticos generales de la nueva Comisión Europea, resulta crucial resaltar cómo la atención y la manipulación se han convertido en activos económicos clave para los operadores tecnológicos. Estas multinacionales obtienen valor de cualquier interacción que los usuarios tienen con las aplicaciones, redes sociales o, en un sentido más amplio, plataformas digitales.

A lo largo de estos años, los servicios digitales se han nutrido de los datos personales que proporcionamos al registrarnos —como condición para acceder al servicio— o mediante la navegación, *i.e.* por el rastreo y seguimiento a través de las *cookies*[36]. Esto les ha permitido adquirir un conocimiento detallado sobre nuestros hábitos, comportamientos, preferencias e incluso vulnerabilidades, colocándoles significativamente en una situación privilegiada para influir en nuestras decisiones. De hecho, alguna

36. Aunque muchos servicios ofrecidos en el entorno digital se presentan como gratuitos, en realidad su acceso suele estar condicionado por el modelo "*consent or pay*". Un sistema que ofrece al usuario dos opciones: consentir el tratamiento de sus datos personales —especialmente para fines publicitarios *personalizados*— y acceder gratuitamente al contenido ofrecido por el servicio, o, en caso de no dar este consentimiento, abonar una tarifa para poder utilizar el servicio. Sobre este aspecto, véase, TRUJILLO CABRERA, C.: "Los nuevos cookie walls: 'consent or pay'. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023", *Revista de Derecho Civil*, vol. XI, núm. 2, 2024, págs. 75-112; DAVIES, G.: "Consent or Pay: Transforming Internet Users from Products into Customers", *Journal of European Consumer and Market Law*, vol. 14, núm. 1, 2025, págs. 6-14; GASCÓN MARCÉN, A.: El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea, *Cuadernos de derecho transnacional*, vol. 13, n.º 2, 2021, págs. 209-232.

voz subraya que "la privacidad desempeña un papel en la vulnerabilidad digital"[37].

En términos generales, puede sostenerse que los usuarios no ejercemos plena soberanía en nuestras decisiones digitales. Ya sea por pasividad, aquiescencia o desconocimiento, los usuarios proporcionamos a las tecnológicas constante información valiosa sobre nuestros comportamientos en línea. Esta forma de vigilancia comercial, basada en la recolección y segmentación de nuestros datos por el rastro digital (en su mayor parte imperceptible para el usuario), es utilizada hábilmente para predecir, moldear y rentabilizar nuestras acciones. A cambio, se nos ofrece una experiencia digital personalizada e intuitiva, mientras estas compañías obtienen extraordinarios beneficios económicos[38].

En este contexto, cuanto más tiempo permanezcamos conectados a internet, mayor es la rentabilidad generada. Por ello, uno de los desafíos actuales es cómo abordar la comercialización de nuestra atención.

Como se ha referido, la cuadratura del círculo en materia de regulación digital parece situarse en cómo solventar los efectos perjudiciales que generan las plataformas digitales por el uso de técnicas deliberadamente diseñadas para manipular y captar la atención continua del usuario.

Los esfuerzos del legislador de la Unión Europea por construir un ecosistema digital más transparente y confiable son, sin duda, loables, como lo refleja el marco normativo vigente orientado en esa dirección. Sin embargo, aún persisten retos significativos para lograr un entorno digital verdaderamente justo y equitativo. En este contexto, fenómenos como la

---

37. DOMURATH, I.: "Digital Vulnerability as a Power Relation" en CREA, C. y DE FRANCESCHI, A. (eds.): *The New Shapes of Digital Vulnerability in European Private Law*, nomos, 2024, pág. 244.

38. Señala el informe realizado por la organización europea de consumidores BEAUC que "[…] uno de los problemas fundamentales de la protección de los consumidores en el ámbito digital es la existencia de enormes asimetrías digitales en forma de control sobre los datos, el conocimiento, las infraestructuras y los potentes modelos algorítmicos optimizados para maximizar los beneficios, los clics, el compromiso, la adicción y la dependencia. Los consumidores se benefician sin duda de una gran cantidad de nuevas aplicaciones y servicios, de la facilidad de integración, de las plataformas transfronterizas y de la personalización sin esfuerzo. Sin embargo, este nuevo nivel de comodidad para el cliente tiene un precio, en forma de pérdida de control, pérdida de privacidad, nuevas formas de adicción, susceptibilidad a la manipulación y dependencias estructurales […]". HELBERGER, H. y otros, *Digital Fairness for Consumers*, BEAUC, 2024, pág. 259.

ansiedad derivada del uso compulsivo de redes sociales, la disminución de la autoestima por la escasez de reacciones positivas (como "me gusta" o *likes*), el consumo prolongado y excesivo de contenidos durante horas, o el sentimiento de haber sido manipulado (o engañado) por interfaces diseñadas para incidir indebidamente en la toma de decisiones del usuario, revelan los peligros de una economía digital estructurada en torno a la monetización de nuestra atención, a través de prácticas que, por su impacto potencial sobre los derechos de los usuarios, deberían estar sujetas a una regulación más exhaustiva, o al menos, a mayores estándares de transparencia que posibiliten a los usuarios ejercer un consentimiento realmente informado.

Efectivamente, las grandes corporaciones tecnológicas juegan con ventaja. En un contexto donde la información abunda de forma casi ilimitada en internet, captar y retener la atención del usuario se ha convertido en una prioridad. La atención es un recurso escaso, convertido en una valiosa mercancía. Así, estos gigantes —como por ejemplo el conglomerado tecnológico Meta o la red social X— no obtienen directamente sus ingresos de los usuarios, sino de comercializar su atención. Esta se convierte en el producto esencial que se vende a terceros, principalmente anunciantes u otros actores económicos interesados en datos sobre el comportamiento del usuario. Y como se ha referido, el modelo económico dominante en el entorno digital se basa en la explotación sistemática de nuestra atención.

En esta economía de la atención, nada se deja al azar: se desarrollan entornos digitales diseñados para maximizar el tiempo de exposición del usuario, mediante estrategias adictivas y personalizadas. Cuanto más prolongada es la interacción, mayor es la cantidad de datos generados y más altos son los beneficios económicos obtenidos. Los algoritmos y otras herramientas de predicción permiten adaptar los estímulos y contenidos a cada usuario, con el objetivo de aumentar su implicación y permanencia en el servicio digital.

Y si bien la legislación sectorial de la Unión Europea ha comenzado a establecer límites, en particular a través del Reglamento (UE) 2022/2065 de servicios digitales, así como mediante otras normativas[39], imponiendo obligaciones a las plataformas en línea —y su efecto es absolutamente posi-

39. Como, por ejemplo, el Reglamento (UE) 2016/679 General de Protección de Datos, el Reglamento (UE) 2022/1925 de mercados digitales, el Reglamento (UE) 2024/1689 de inteligencia artificial; y también estos límites pueden encontrarse en la Directiva 2005/29/CE sobre prácticas comerciales desleales, la Directiva 93/13/CEE sobre las cláusulas abusivas en los contratos celebrados con consumidores; la Directiva 2011/83/UE sobre los derechos de los consumidores.

tivo—, todavía queda camino por recorrer para mitigar la explotación de las vulnerabilidades de los consumidores y usuarios en el entorno digital.

2. MEDIDAS DISEÑADAS PARA MITIGAR LAS TÉCNICAS DE MANIPULACIÓN Y ADICCIÓN DE LAS PLATAFORMAS DIGITALES

El recurso a técnicas de manipulación y persuasión por parte de los operadores económicos con el fin de incidir en las decisiones de los consumidores es una práctica bien consolidada. Tradicionalmente, tanto las campañas de marketing en medios de comunicación convencionales —radio, prensa o televisión— como las estrategias aplicadas por avispados vendedores de comercios y de grandes superficies han buscado influir el comportamiento del consumidor hacia determinados productos o servicios. No obstante, cualquiera de estas prácticas adquiere una dimensión significativamente mayor en el entorno digital, debido al vasto volumen de datos que las multinacionales tecnológicas recopilan a partir de nuestra huella digital.

Esta información les permite perfeccionar sus mecanismos de influencia de forma cada vez más sofisticada, sutil y, en la mayoría de las ocasiones, difícilmente perceptible para el usuario medio.

A este respecto, un estudio realizado por la Comisión Europea evidencia que el noventa y siete por ciento de los sitios web y aplicaciones más utilizados por los consumidores en la Unión emplean, al menos, un patrón oscuro[40].

---

40. Los patrones oscuros son estrategias digitales que afectan negativamente la capacidad de decisión de los consumidores al diseñar las opciones de manera que los influencian. Utilizados en las interfaces en línea, estos mecanismos pueden inducir, confundir o presionar a los usuarios para que elijan alternativas contrarias a sus propios intereses. Entre las prácticas más comunes destacan: la ocultación de información relevante, la estructuración engañosa de las alternativas ofrecidas, la reiteración persistente de una misma petición, la complicación del proceso para anular servicios y la exigencia de un registro obligatorio. Véase el considerando núm. 67del Reglamento (UE) de servicios digitales en la nota al pie 48. Igualmente, entre otros, *cfr.* OECD, *Dark commercial patterns*, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, 2022; MATO PACÍN, M.N.: *Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros*, Agencia Estatal Boletín Oficial Del Estado, Madrid, 2024 págs. 54-60; CORBERÁ MARTÍNEZ, J., "Diseño y organización de interfaces en línea en el Reglamento (UE) de servicios digitales" en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 171-200; *Id.*, "Evolución de la regulación de los 'Dark Patterns' en la Unión Europea" en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

Asimismo, aproximadamente el cuarenta por ciento de los encuestados afirmó haber experimentado situaciones en las que el diseño o el lenguaje empleado en una página web —o aplicación— inducía confusión, impidiéndoles comprender con claridad los términos aceptados, así como sus derechos y obligaciones. Por otro lado, el sesenta y seis por ciento de los usuarios señaló haber recibido mensajes indicando escasa disponibilidad del producto o una alta demanda simultánea por parte de otros consumidores, mientras que el sesenta y uno por ciento fue expuesto a afirmaciones de que determinados productos estarían disponibles únicamente por un tiempo limitado. En ambos casos, no existía posibilidad de verificar la veracidad de dicha información.

Un treinta y dos por ciento de los encuestados manifestó haber pagado un importe superior al inicialmente anunciado debido a variaciones en el precio durante el proceso de compra. De igual forma, casi la mitad indicó haber sido presionados con reiterativos mensajes para tomar decisiones (como suscribirse a servicios *premium*, aceptar descuentos especiales o adquirir productos recomendados). Incluso tras haber manifestado su elección o rechazo a la oferta, el cuarenta y dos por ciento recibió mensajes diseñados para generar duda o incertidumbre respecto a su decisión, con preguntas de si estaba realmente seguro de no querer aprovechar un descuento. Un treinta y siete por ciento reconoció haber encontrado información relevante que estaba visualmente oculta o presentada de forma que se destacaban opciones menos beneficiosas. Este mismo porcentaje detectó que ciertas configuraciones predeterminadas favorecían a la empresa, dificultando su modificación. Y un cuarenta y dos por ciento de los consumidores mencionó situaciones en las que la opción seleccionada condujo a un resultado distinto al esperado: por ejemplo, al hacer clic para darse de baja los redirigía a una página con mensajes disuasivos destacando los beneficios del servicio que se perdería, dilatando o dificultado la acción deseada.

En todos estos supuestos, las prácticas engañosas y manipuladoras se articulan mediante herramientas tecnológicas —particularmente a través del uso de los referidos patrones oscuros— con el objetivo de influir en la toma de decisiones del usuario, favoreciendo de manera sistemática los intereses del operador tecnológico.

La personalización o curación —algorítmica— de contenidos constituye otro elemento esencial en el modelo de negocio de las grandes plataformas tecnológicas[41]. En términos generales, los sistemas de recomendación auto-

41. Un estudio completo de los sistemas de recomendación, *vid*., GENOVESI, S.; KAESLING, K. y ROBBINS, S. (ed.): *Recommender Systems: Legal and Ethical Issues*, Springer, 2023, *passim*.

matizados se encargan de filtrar, ordenar, clasificar y priorizar la información conforme a los intereses y preferencias del usuario, influyendo de manera decisiva en su acceso e interacción con determinados contenidos digitales. De acuerdo con el señalado estudio de la Comisión, reveló que el treinta y siete por ciento de los consumidores tenía la impresión de que el operador económico conocía sus vulnerabilidades y las utilizaba con fines comerciales. Asimismo, el setenta y cuatro por ciento de los consumidores consideraba que sus datos personales se habían utilizado de forma indebida o injusta para personalizar ofertas comerciales en el último año[42].

Esta personalización no solo optimiza la experiencia de navegación al facilitar el acceso a información considerada relevante en un mundo saturado de información —mientras relega otra[43]—, sino que también promueve un uso más frecuente y prolongado del usuario en el servicio digital, lo que se traduce, como se viene señalando, en mayores beneficios económicos derivados de la extracción y explotación de sus datos personales. Si bien estos sistemas mejoran significativamente la experiencia digital del usuario al ofrecer contenidos ajustados a sus gustos, su funcionamiento no está exento de implicaciones problemáticas.

En este sentido, uno de sus efectos es la creación de burbujas de filtro[44], esto es, entornos informativos cerrados (o restringidos) en los que el algoritmo tiende a mostrar de forma predominante información que coincide con las preferencias previamente expresadas por el usuario. Este fenómeno reduce significativamente la diversidad informativa a la que se expone el usuario

---

42. *Vid*., Documento de Trabajo de la Comisión *Fitness Check of EU consumer law on digital fairness*, Bruselas, 3.10.2024. SWD (2024) 230 final, págs. 21 y 22.
43. Sobre la relevancia del lugar que ocupa esta información, véase, CASTELLÓ PASTOR, JJ.: "Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 361-394; LAPIEDRA ALCAMI, R.: "Hacia la transparencia y la equidad en el 'ranking' de resultados a la luz del Reglamento 2019/1150", en *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi Thomson Reuters, 2021, págs. 161-193.
44. PARISER, E.: *The filter bubble: What the internet is hiding from you*, Penguin Press, 2011. TORNADA, J., "How (Not) To deal with the Bubble Effect in Cyberspace: The Case of the EU and Digital Services Act", *Brook. J. Int´l L.*, vol. 49, 2024, págs. 97-131; e igualmente véase el apartado III. 1.3 de la contribución de CORDERO ÁLVAREZ, C.I.: "Inteligencia artificial y riesgos sistémicos en la red: la lucha contra la desinformación en la Unión Europea", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

digital, favoreciendo la reiteración de contenidos, la amplificación de determinados discursos, la viralización de contenidos similares y la promoción de conductas alineadas con los patrones de consumo digital del usuario. Como consecuencia, se produce una exclusión sistemática de puntos de vista alternativos o disonantes. Por consiguiente, el usuario tiende a quedar inmerso en una suerte de *bucle* de retroalimentación informativa, donde únicamente se les ofrece contenidos afines a sus preferencias previas, distanciándose de otras opciones y, a largo plazo, contribuye a una creciente polarización social[45].

Por otro lado, conviene subrayar que, si bien la eficacia de la personalización permite al usuario acceder con mayor facilidad a contenidos que se ajustan a sus preferencias, esta funcionalidad plantea inquietudes al legislador, especialmente en lo relativo a los sistemas de recomendación basados en la interacción del usuario y a las notificaciones que reciben, por la adicción que puede generar. De hecho, existe una creciente preocupación por el riesgo de que estos mecanismos fomenten patrones adictivos, agravado por el diseño de las interfaces en línea que actúan como estímulos para retener la atención del usuario, bien por el diseño adictivo bien por la incorporación de los mencionados patrones oscuros.

Estos datos del estudio elaborado por la Comisión Europea muestran que, pese a los avances significativos introducidos por el Reglamento (UE) 2022/2065 de servicios digitales y por otras normativas aplicables al ecosistema digital[46], aún persiste un amplio margen de mejora en la regulación de determinadas prácticas en la red.

Sin entrar en un análisis exhaustivo del contenido normativo del mencionado Reglamento (UE) 2022/2065 de servicios digitales[47], cabe destacar —en lo que respecta al ámbito de interés de este epígrafe— que este instrumento sustantivo digital prohíbe a las plataformas en línea, regulando por primera vez de forma expresa, el uso de los patrones oscuros[48], en tanto que distor-

45. NEUDERT, L.M. & MARCHAL, M.: *Polarisation and the use of technology in political campaigns and communication*, EPRS, 2019, págs. 15-29.

46. Como el Reglamento (UE) 2022/2065 de Servicios Digitales, el Reglamento (UE) 2022/1925 de mercados digitales y el Reglamento (UE) 2024/1689 de inteligencia artificial, además del Reglamento (UE) 2023/2854 de Datos y la Directiva (UE) 2018/1808 sobre Servicios de Medios Audiovisuales, entre otras. Estos instrumentos complementan la protección de los consumidores de la Unión Europea.

47. Véase la obra colectiva, *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, Cizur Menor, 2024.

48. El considerando 67 del Reglamento (UE) de servicios digitales se refiere algunos de ellos. En este sentido señala que "las interfaces engañosas de las plataformas en línea

sionan las decisiones de los destinatarios del servicio[49]. Asimismo, aborda otro aspecto fundamental: la publicidad en las plataformas en línea. Esta se regula fundamentalmente a través de un principio básico, la transparencia,

son *prácticas que distorsionan o merman sustancialmente, de forma deliberada o efectiva, la capacidad* de los destinatarios del servicio de tomar decisiones autónomas y con conocimiento de causa. Estas prácticas pueden utilizarse para persuadir a los destinatarios del servicio de que adopten comportamientos no deseados o decisiones no deseadas que tienen consecuencias negativas para ellos. Por esta razón, debe prohibirse a los prestadores de plataformas en línea *engañar o empujar en esta dirección* a los destinatarios del servicio *y distorsionar u obstaculizar la autonomía, la toma de decisiones o la capacidad de elección de los destinatarios del servicio a través de la estructura, el diseño o las funcionalidades de una interfaz en línea o una parte de esta*. Entre estas prácticas se han de incluir, entre otras, las *opciones de diseño abusivas* que dirigen al destinatario hacia acciones que benefician al prestador de plataformas en línea, pero que pueden no favorecer los intereses de los destinatarios, al *presentar opciones de una manera que no es neutra*, por ejemplo, dando más protagonismo a determinadas opciones mediante componentes visuales, auditivos o de otro tipo, cuando se le pide al destinatario del servicio que tome una decisión. Otras prácticas que también deben estar incluidas son *solicitar repetidamente al destinatario del servicio que tome una decisión cuando esa decisión ya ha sido tomada*, hacer que el *procedimiento de anulación de un servicio sea considerablemente más engorroso* que la suscripción a dicho servicio, hacer que determinadas opciones sean más difíciles o lleven más tiempo que otras, dificultar excesivamente la interrupción de las compras o la desconexión de una plataforma en línea determinada que permite a los consumidores celebrar contratos a distancia con comerciantes, y engañar a los destinatarios del servicio empujándoles a tomar decisiones sobre transacciones o mediante ajustes por defecto que sean muy difíciles de cambiar, dirigiendo de forma injustificada la toma de decisiones del destinatario del servicio, de manera que se distorsione y merme su autonomía, su toma de decisiones y su capacidad de elección. Sin embargo, las normas contra las interfaces engañosas no deben entenderse en el sentido de que impidan a los prestadores interactuar directamente con los destinatarios del servicio y ofrecerles servicios nuevos o adicionales. Las prácticas legítimas, como las publicitarias, que sean conformes con el Derecho de la Unión no deben considerarse en sí mismas interfaces engañosas. Dichas normas sobre interfaces engañosas deben interpretarse en el sentido de que se aplican a las prácticas prohibidas que entran en el ámbito de aplicación del presente Reglamento en la medida en que no estén ya cubiertas por la Directiva 2005/29/CE o el Reglamento (UE) 2016/679" (énfasis añadido).

49. Conforme al artículo 25 sobre el diseño y organización de interfaces en línea: "1. Los prestadores de plataformas en línea no diseñarán, organizarán ni gestionarán sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas […]". Sobre esta disposición, véase CORBERÁ MARTÍNEZ, J., "Diseño y organización de interfaces en línea en el Reglamento (UE) de servicios digitales" en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 171-200; *Id*., "Evolución de la regulación de los 'Dark Patterns' en la Unión Europea" en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

que se concreta con diversas obligaciones. Por un lado, se exige un repositorio de anuncios; por otro, se impone la obligación de garantizar que el destinatario del servicio pueda identificar cuándo está ante un contenido publicitario. Para ello, se les obliga a incorporar etiquetas visibles, identificar al anunciante y los principales parámetros utilizados para dirigirse a los destinatarios[50]. De manera adicional, se prohíbe expresamente la publicidad dirigida a menores, como también la basada en datos personales de carácter sensible[51]. Del mismo modo, las plataformas deben incluir una funcionalidad que permita a los usuarios —como los conocidos *influencers*— señalar que el contenido difundido incorpora comunicaciones de naturaleza comercial.

Sobre los sistemas de recomendación de contenidos empleados por las plataformas en línea y motores de búsqueda[52], en términos generales, se establece la obligación de que los intermediarios que utilicen este tipo de sistemas informen, de forma clara y comprensible, en sus condiciones generales, sobre los principales parámetros que rigen su funcionamiento, así como sobre las opciones disponibles para que los destinatarios del servicio puedan personalizarlos o ajustarlos a sus preferencias. Sin embargo, pese a la loable intención del legislador de promover la transparencia informativa, desde mi punto de vista, esta exigencia presenta limitaciones prácticas. En efecto, para los usuarios que no posean conocimientos técnicos especializados, resulta particularmente complejo comprender en profundidad el funcionamiento de estos mecanismos, aun cuando la información ofrecida se redacte en términos accesibles. La mera transcripción en lenguaje claro y comprensible de los parámetros utilizados y de las posibles opciones de configuración no garantiza, necesariamente, una comprensión efectiva o un uso consciente por parte del destinatario del servicio. Por otro lado,

50. *Vid*. artículo 26 Reglamento (UE) de servicios digitales. Publicidad en las plataformas en línea.

51. Sobre estas obligaciones, véase, en relación con la publicidad, LAPIEDRA ALCAMÍ, R., "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad digital" en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 205-226; *Id*.: "Hacia un entorno digital seguro para la infancia: el marco europeo y estatal de protección de los menores", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

52. Se abordan en el artículo 27 del Reglamento (UE) de servicios digitales. Sobre los sistemas de recomendación, véase CASTELLÓ PASTOR, JJ.: "Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 361-394.

el artículo 38 del Reglamento establece obligaciones adicionales para las plataformas en línea y los motores de búsqueda de muy gran tamaño que utilicen estos sistemas de recomendación. En concreto, se exige que proporcionen al usuario, al menos, una opción que no se base en la elaboración de perfiles ni en la monitorización de su comportamiento en línea. Esta disposición introduce, en la práctica, un mecanismo de *opt-out*, otorgando al usuario la capacidad de decidir si desea interactuar con contenidos sugeridos mediante sistemas personalizados, o bien optar por recomendaciones no perfiladas[53].

Asimismo, se impone a las grandes plataformas en línea y buscadores la obligación específica de mitigar los riesgos sistémicos, entre los que destaca la necesidad de llevar a cabo un identificación, análisis y evaluación exhaustiva de los riesgos que puedan derivarse del diseño, funcionamiento o uso de sus servicios. Estos riesgos comprenden, entre otros, aquellos susceptibles de generar un impacto negativo, real o previsible, sobre, por ejemplo, la protección de los consumidores y los derechos del menor. En función de los riesgos detectados, deben implementar medidas de mitigación que sean razonables, proporcionales y eficaces, entre las que podrían incluirse desde ajustes en el diseño de sus servicios o interfaces, hasta cambios en los términos y condiciones, campañas de sensibilización o la incorporación

53. El artículo 38 del Reglamento (UE) de servicios digitales ha sido objeto de análisis por parte del Tribunal de General en el asunto T-367/23 *Amazon Services Europe/Comisión* (EU:T:2023:589) de 27 de septiembre de 2023, con motivo de la solicitud de medidas provisionales por Amazon en relación con la suspensión de la aplicación de la Decisión de la Comisión sobre las obligaciones impuestas a Amazon Store en virtud del artículo 38 (y 39) del Reglamento (UE) de servicios digitales. En síntesis, el gigante tecnológico argüía que la obligación de ofrecer una opción de exclusión voluntaria para sus sistemas de recomendación dará lugar a una reducción significativa y pérdida irreversible de cuota de mercado, que le causará un daño grave e irreparable, además de obligarla a modificar una de las piezas fundamentales del software en el que se basa su negocio, con efectos negativos inmediatos y graves en las experiencias de compra de los clientes. Y ello conducirá a una desventaja competitiva significativa en comparación con los mercados en línea y los minoristas que no están designados como plataformas en línea muy grandes (punto 28 y 29), toda vez que si no se personaliza esta información se mostrarán productos de escasa relevancia para los clientes, lo que, a su modo de ver, socavará la función principal de los *marketplaces* (punto 30). Afirma, además, que el usuario no entenderá esta función pero que atribuirá a la plataforma el impacto de su exclusión voluntaria por su mala experiencia que implicará posiblemente una reducción de su presencia en el uso de la tienda de Amazon (punto 31) y, por tanto, una irreparable pérdida de cuota de mercado además de perjudicar también a los intereses de los terceros vendedores que usan Amazon Store. El Tribunal, sin embargo, desestima la petición porque la tecnológica no demuestra este perjuicio grave e irreparable alegado.

de salvaguardias específicas dirigidas a grupos o colectivos en situación de vulnerabilidad[54].

IV. EQUIDAD DIGITAL: PATERNALISMO DEL REGULADOR VS. SOBERANÍA DEL CONSUMIDOR

El marco jurídico digital establecido en los últimos años ha contribuido de manera positiva a la salvaguarda de los derechos de los consumidores y usuarios en el entorno digital. No obstante, tal como se ha señalado, aún subsisten ciertas carencias en este *corpus* normativo vigente que dificultan una protección adecuada de los grupos más vulnerables, comprometiendo así una tutela efectiva y segura de sus derechos digitales en un panorama tecnológico en constante transformación.

La Resolución del Parlamento Europeo sobre el diseño adictivo de los servicios en línea, adoptada en el año 2023, subrayó las consecuencias perjudiciales que estas prácticas pueden tener para los consumidores, particularmente para los más jóvenes. En esta misma línea, los resultados de la iniciativa del *Digital Fairness — Fitness Check on EU Consumer Law* de la Comisión Europea presentados el 4 de octubre de 2024, evidencian cómo las dinámicas de las plataformas digitales pueden minar la autonomía de los consumidores y usuarios mediante prácticas comerciales ciertamente

54. Véase CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, Vol. 17, n.º 1, 2025, págs. 308-328; GASCÓN MARCÉN, A.: "La diligencia debida en los Reglamentos de Servicios Digitales e Inteligencia Artificial" en *Empresa y derechos humanos: retos y tendencias normativas ante un complejo e inédito contexto geoestratégico* (Dir. ÁLVAREZ RUBIO, J.J.), Aranzadi, 2025, págs. 235-243; REIG FABADO, I., "Las VLOPS y los riesgos sistémicos en la DSA: algunos aspectos problemáticos", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, Cizur Menor, 2024, págs. 289-322; *Id*., "Inteligencia Artificial y tutela jurídica de derecho digitales en la UE" en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025; CORDERO ÁLVAREZ, C.I.: "Inteligencia artificial y riesgos sistémicos en la red: la lucha contra la desinformación en la Unión Europea", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025; Id., "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 69-105; PLA ALMENDROS, R., *La solución extrajudicial de disputas transfronterizas en el Reglamento de Servicios Digitales*, Colex, A Coruña, 2025.

desleales, el uso de diseños o funcionalidades que fomentan la adicción digital, comprometiendo, en definitiva, la confianza en el ecosistema digital.

La relación entre las plataformas en línea y sus usuarios se encuentra marcada por una notoria asimetría estructural[55]. Mientras que las primeras, como se ha señalado, destinan considerables recursos a diseñar estrategias orientadas a la captación y retención de la atención con el fin último de maximizar sus beneficios económicos, los usuarios nos vemos inmersos en dinámicas complejas que, en muchas ocasiones, exceden de nuestra capacidad o control efectivo.

Esta desigualdad estructural en el ecosistema digital pudiera justificar, una vez más, la pertinencia de una intervención del regulador que incorpore medidas correctoras orientadas a garantizar una protección efectiva de todos los usuarios, independientemente de su nivel de alfabetización tecnológica.

De ello se ocupará la futura *Ley* de equidad digital. Aunque sólo se dispone de información limitada, anticipándose la publicación de la propuesta legislativa para el primer trimestre de 2026[56], la Comisión Europea tiene la intención de regular prácticas comerciales poco éticas vinculadas a los patrones oscuros, a la publicidad de los *influencers*, al diseño adictivo de productos digitales y a la elaboración de perfiles en línea, especialmente en aquellos casos en que se aprovechan las vulnerabilidades de los consumidores con fines comerciales.

Más allá de la importancia que tendrá esta futura norma sobre la equidad digital[57], a mi modo de ver, considero fundamental que el instrumento jurídico adoptado sea un Reglamento. Esto permitirá evitar la fragmentación legislativa en el seno de la Unión Europea, asegurando un marco normativo uniforme y de obligado cumplimiento para todos los actores tecnológicos, incluidos aquellos establecidos fuera del territorio de la Unión. Esta elec-

---

55. GOANTA, C., DE GREGORIO, G., SPANAKIS, J.: "Consumer Protection and Digital Vulnerability: Common and Diverging Paths", en CREA, C. y DE FRANCESCHI, A. (eds.): *The New Shapes of Digital Vulnerability in European Private Law*, nomos, 2024, págs. 34 y ss.

56. Se ha anunciado una consulta pública para que los ciudadanos, autoridades públicas y cualquier parte interesada pueda compartir sus ideas sobre cómo seguir reforzando la protección de los consumidores en el entorno digital (de acuerdo con la información disponible en: ec.europa.eu).

57. Aunque la vaguedad intrínseca de este concepto de equidad digital podría convertirse en un obstáculo para garantizar una aplicación uniforme en los mercados digitales. *Vid.*, NIKIFOROV, L.: *Digital Fairness Act: If and How*, Brussels Privacy Hub, 2024 (disponible en: brusselsprivacyhub.com), pág. 5.

ción se justifica por el carácter intrínsecamente transfronterizo de internet, que exige un criterio de conexión fáctico, como el utilizado en recientes normativas digitales. Así, el ámbito de aplicación territorial de la futura *Digital Fairness Act* debería abarcar a todos los operadores económicos que presten u ofrezcan sus servicios en la Unión Europea, con independencia del lugar de su sede, domicilio o establecimiento[58]. Además, sería deseable que este nuevo marco regulatorio incorpore mecanismos tanto de supervisión pública como de tutela jurídico-privada que garanticen de forma efectiva el cumplimiento de sus objetivos[59].

Entrando en el meollo de lo que parece ser objeto de regulación de la futura *Digital Fairness Act* y aunque resulta loable su objetivo, orientado a la protección de los consumidores —con especial atención a colectivos vulnerables como menores y adolescentes, quienes representan un segmento particularmente expuesto en el ecosistema digital—, conviene subrayar que esta iniciativa no nace en un vacío normativo. En efecto, la *Digital Fairness Act* se integrará de manera complementaria en el mencionado *corpus* jurídico digital de la Unión Europea[60], en particular con el Reglamento (UE) 2022/2065 de Servicios Digitales. No obstante, su alcance parece proyectarse más allá de los prestadores de servicios de intermediación (porque muchas de las apps, tiendas y juegos en línea quedan fuera de su ámbito material), extendiéndose así a los operadores económicos digitales que actúan en el

58. De acuerdo con el artículo 2.1 del Reglamento (UE) de servicios digitales. Con mayor profundidad, FELIU ÁLVAREZ SOTOMAYOR, S., "Ámbito territorial y aplicación del principio del control en origen en el Reglamento UE de servicios digitales", en CASTELLÓ PASTOR, J.J. (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, págs. 41-64. Igualmente, véase, CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, Vol. 17, n.º 1, 2025, págs. 316-317 en el que cuestiono si estamos ante un proteccionismo encubierto dado el carácter imperativo de las reglas del Reglamento (UE) de servicios digitales a las tecnológicas situadas en terceros Estados.

59. *Vid*. CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, Vol. 17, n.º 1, 2025, págs. 317-322 en el particular "David c. Goliat: tutela jurídico-pública y privada del nuevo marco jurídico-digital".

60. Entre otras, como se ha referido anteriormente, el Reglamento (UE) 2016/679 General de Protección de Datos, el Reglamento (UE) 2022/1925 de mercados digitales, el Reglamento (UE) 2024/1689 de inteligencia artificial. Y en el marco de protección de los consumidores, por ej., la Directiva 2005/29/CE sobre prácticas comerciales desleales, la Directiva 93/13/CEE sobre las cláusulas abusivas en los contratos celebrados con consumidores; la Directiva 2011/83/UE sobre los derechos de los consumidores.

mercado interior, lo que evidencia su vocación más expansiva. Esta futura normativa debería ser horizontalmente aplicable a todas las relaciones B2C, independientemente del sector[61].

Cabe cuestionarse, en este punto, si es necesario adoptar una nueva legislación sectorial, con un enfoque claramente proteccionista por parte del regulador de la Unión Europea, o si es suficiente con fortalecer la aplicación —rigurosa y eficaz— del acervo normativo vigente, atendiendo a las deficiencias puestas de manifiesto en el documento *Digital Fairness — Fitness Check on EU Consumer Law*. Esta última podría venir reforzada con la publicación de directrices que orienten su implementación práctica. Muestra de ello son las recientes Directrices sobre medidas para garantizar un alto nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065 de servicios digitales[62].

No faltan voces que advierten, con razón, que una sobrerregulación legislativa podría traducirse en una restricción del potencial innovador del sector tecnológico[63]. En este sentido, se apunta también que no solo podría resultar redundante, sino también incrementar de forma innecesaria la complejidad al marco jurídico vigente. En efecto, el marco normativo vigente ya abarca en gran medida las conductas o prácticas relevantes de los actores tecnológicos[64]. En este sentido, en lo que respecta a los patrones oscuros, se subraya la existencia de diversas disposiciones recogidas en el ordenamiento jurídico de la Unión Europea. En particular, la Directiva 2005/29/CE sobre prácticas comerciales, incluido su anexo de prácticas prohibidas. De forma

---

61. Así lo indica Namysłowska, que además subraya que "un enfoque sectorial es insuficiente en un ecosistema digital en el que las plataformas lo median todo, desde la búsqueda de productos hasta el consumo de contenidos. Las actividades en un ámbito (como la publicidad) influyen directamente en el comportamiento en otro (como el comercio electrónico o las suscripciones). Un marco horizontal garantiza la coherencia jurídica y colma las lagunas derivadas de una regulación aislada" (traducción del autor). NAMYSŁOWSKA, M.: "The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices", *Journal of Consumer Policy*, 2025 (versión en línea).
62. Bruselas, 14.7.2025 C (2025) 4764 final.
63. *Vid*. NIKIFOROV, L.: *Digital Fairness Act: If and How*, Brussels Privacy Hub, 2024, págs. 5 y 6.
64. Un conjunto de asociaciones que agrupan a empresas de diversa índole, tanto por tamaño como por sector de actividad, ha emitido la declaración "Un llamamiento a favor de políticas orientadas a la competitividad" ciertamente interesante (disponible en: https://doteurope.eu/wp-content/uploads/2025/06/Joint-industry-statement-on-the-Digital-Fairness-Act.pdf).

complementaria, como se ha referido, el Reglamento (UE) 2022/2065 de servicios digitales introduce disposiciones dirigidas a las plataformas en línea, mientras que el Reglamento (UE) 2016/679 General de Protección de Datos establece requisitos en torno al consentimiento, su obtención y revocación, configurándose como una salvaguarda clave frente a estas prácticas engañosas. Finalmente, el Reglamento (UE) 2024/1689 de inteligencia artificial incorpora una prohibición expresa del uso de técnicas subliminales que puedan modificar de manera sustancial el comportamiento de las personas, lo que refuerza el marco de protección frente a estos mecanismos[65].

Con respecto a la personalización —los sistemas de recomendación y la publicidad dirigida—, el marco jurídico de la Unión Europea contempla diversas disposiciones aplicables. Estas prácticas están reguladas principalmente por el Reglamento (UE) 2016/679 General de Protección de Datos, la Directiva 2002/58/CE sobre privacidad electrónica y el Reglamento (UE) 2022/2065 de servicios digitales. Entre sus disposiciones destacan la prohibición de publicidad dirigida a menores de edad, el uso de datos personales sensibles para fines comerciales y el reconocimiento del derecho de los usuarios a acceder a sistemas de recomendación que no se basen en perfiles conductuales[66].

En lo relativo al diseño adictivo, este se encuentra regulado principalmente por el Reglamento (UE) 2022/2065 de servicios digitales, en el marco de las obligaciones vinculadas a la evaluación de riesgos sistémicos, así como por sus disposiciones sobre sistemas de recomendación basados en perfiles. Por otro lado, en materia de suscripciones, el marco normativo vigente —*i.e.* la Directiva 2011/83/UE sobre los derechos de los consumidores, la Directiva 2005/29/CE sobre prácticas comerciales y el Reglamento (UE) 2022/2065 de servicios digitales— contempla medidas orientadas a proteger al consumidor frente a prácticas que dificultan la cancelación de la suscripción o la baja del servicio digital. Finalmente, en el ámbito del marketing de *influencers*, el marco normativo de la Unión contempla un conjunto de normas —*cfr.* la Directiva 2005/29/CE sobre prácticas comerciales, la Directiva (UE) 2018/1808 sobre servicios de comunicación audiovisual y el Reglamento (UE) 2022/2065 de servicios digitales— orientadas a garantizar la transparencia e información de contenidos patrocinados, la prohibición de la publicidad encubierta y el etiquetado claro de anuncios y recomendaciones[67]. En este contexto, señalan, el papel del *Influencer Legal Hub* impul-

65. *Ibid.*
66. *Ibid.*
67. *Ibid.*

sado por la Comisión Europea[68], que ofrece directrices actualizadas para la correcta aplicación de estas normativas.

En todo caso, en los próximos meses veremos cómo se desarrolla el proceso de consulta pública y la elaboración de la propuesta legislativa, especialmente si los actores tecnológicos —a través de sus *lobbies*— señalan un posible conflicto entre una regulación exhaustiva de los patrones oscuros y ciertos derechos fundamentales —como el de los operadores económicos a diseñar libremente sus modelos de negocio, amparado por la libertad de empresa reconocida en el artículo 16 de la Carta de los Derechos Fundamentales de la Unión Europea—[69].

Este futuro texto adoptado por las instituciones de la Unión podría, en ciertos aspectos, interpretarse como una forma de paternalismo digital que —si bien puede estar justificado en la protección del consumidor frente a prácticas— también plantea interrogantes sobre el alcance del regulador en la configuración de las dinámicas comerciales del entorno digital. En este sentido, es preciso mantener una visión crítica, que considere, por una parte, la capacidad de las grandes plataformas tecnológicas para utilizar sus recursos con el fin de maximizar ingresos, y por otra, la importancia de que una excesiva regulación no termine por obstaculizar la innovación ni menoscabar los derechos fundamentales de los agentes económicos[70]. Respetando, en todo caso, la debida salvaguarda de los derechos de los consumidores como su propia autonomía.

En suma, la asimetría digital entre los grandes operadores digitales y los consumidores y usuarios justifica, al menos en principio, que se refuercen nuestros derechos en tanto que parte más débil de la relación. Este enfoque intervencionista busca reequilibrar una relación caracterizada por la desigualdad, acentuada, además, por el desconocimiento generalizado sobre el funcionamiento de las tecnológicas. Sin embargo, no puede pasarse por alto que una sobrerregulación por la Comisión, centrada exclusivamente a la tutela del consumidor, puede proyectar una imagen de paternalismo difícilmente compatible con el ideal del consumidor soberano, históricamente promovido por las propias políticas de la Unión. A mi modo de ver, una protección excesiva del usuario, aunque persiga fines legítimos, puede terminar por minar su capacidad de decisión. Al restringir el margen de

68. *Influencer Legal Hub* (información disponible en: commission.europa.eu).
69. En este sentido, véase KÜHLING, J.: "Digital fairness in online retail", 2024, pp. 26-35, en particular, pág. 30 (estudio disponible en: eurocommerce.eu).
70. *Ibidem*, pág. 86.

libertad y responsabilidad del usuario en la toma de sus decisiones en el entorno digital, se corre el riesgo de infantilizar al usuario, debilitando así su plena capacidad para actuar como sujeto autónomo en el entorno digital.

V. REFLEXIÓN FINAL

Uno de los asuntos más relevantes en el ámbito digital actual es el impacto negativo que pueden ejercer algunas plataformas —ya sean de comercio electrónico, redes sociales u otras— al utilizar técnicas estratégicamente diseñadas para incidir en la conducta de los usuarios digitales y captar de manera sostenida su atención.

En términos generales, puede afirmarse que los usuarios no ejercemos un control soberano pleno sobre nuestras decisiones en el entorno digital. Ya sea por pasividad, conformidad o desconocimiento, contribuimos activamente a que las empresas tecnológicas recojan información valiosa sobre nuestros comportamientos en línea. Esta información, recolectada y sistemáticamente segmentada a partir de nuestra huella digital es utilizada de forma sofisticada para predecir, modelar y monetizar nuestras acciones. A cambio, se nos ofrece una experiencia digital altamente personalizada e intuitiva, mientras estas compañías obtienen réditos económicos extraordinarios.

La aparente sintonía entre los usuarios digitales y las grandes plataformas tecnológicas parece estar llegando a su fin. Distintos indicios, como la ansiedad asociada al uso excesivo de redes sociales, la disminución de la autoestima por la falta de interacciones positivas, el consumo continuo de contenidos digitales o la sensación de haber sido manipulado (o engañado) por diseños que condicionan la toma de decisiones, entre otros tantos, ponen en evidencia los peligros de una economía digital que se sostiene en la comercialización de la atención. Estas prácticas, cuyo efecto sobre los derechos de los consumidores y usuarios es cada vez más notorio, hacen necesaria repensar su regulación o, al menos, una aplicación eficaz de la normativa actual.

Aunque el marco normativo vigente en la Unión Europea ha contribuido de manera notable a generar un entorno digital más seguro, también muestra importantes limitaciones a la hora de abordar de manera eficaz estos daños —presentes y futuros— que afectan a los consumidores. La asimetría digital entre plataformas tecnológicas y usuarios constituye uno de los retos centrales que la Comisión busca corregir con la (¿futura?) *Digital Fairness Act*.

Esta iniciativa, de corte claramente intervencionista, pretende —una vez más— restablecer el equilibrio en una relación estructuralmente asimétrica, intensificada por el desconocimiento generalizado sobre el funcionamiento opaco de estas tecnologías. No obstante, es importante señalar que un enfoque regulatorio excesivamente centrado en la protección del consumidor podría derivar en una visión paternalista, que podría entrar en tensión con el ideal del consumidor soberano, históricamente promovido por las propias políticas de la Unión. Y una protección excesiva del usuario —aunque motivada por fines legítimos— podría, a mi modo de ver, terminar por erosionar su capacidad de decisión. Al restringir su margen de autonomía y responsabilidad, se podría caer en una lógica que infantiliza al usuario, debilitando su plena capacidad para actuar como sujeto autónomo en el entorno digital.

Quizá resulte utópico, pero no por ello menos necesario: tal vez sea oportuno recordar a todos los actores implicados en el ecosistema digital la importancia de fomentar un uso ético, responsable y consciente de internet.

BIBLIOGRAFÍA

AA.VV.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, Cizur Menor, 2024.

BARRIO ANDRÉS, M.: "Inteligencia artificial, Internet de las cosas y blockchain", en *Digitalización y Derecho* (Dir. MONTERO PASCUAL, J.J.), Tirant Lo Blanch, Valencia, 2024.

CASTELLÓ PASTOR, J.J.: "Por un foro de competencia judicial internacional para favorecer al vulnerable de los comportamientos lesivos a los derechos de la personalidad en internet" en *Protección multidisciplinar del vulnerable en la sociedad digital* (Coord. BLANCO GARCÍA, A.I.), Aranzadi, 2024.

CASTELLÓ PASTOR, J.J.: "Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, 2024.

CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, Vol. 17, n.º 1, 2025.

CHRISTAKIS, T.: *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, 2020.

CORBERÁ MARTÍNEZ, J.: "Diseño y organización de interfaces en línea en el Reglamento (UE) de servicios digitales" en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, 2024.

CORBERÁ MARTÍNEZ, J.: "Evolución de la regulación de los 'Dark Patterns' en la Unión Europea", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

CORDERO ÁLVAREZ, C.I.: "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, 2024.

CORDERO ÁLVAREZ, C.I.: "Inteligencia artificial y riesgos sistémicos en la red: la lucha contra la desinformación en la Unión Europea", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

DAVIES, G.: "Consent or Pay: Transforming Internet Users from Products into Customers", *Journal of European Consumer and Market Law*, vol. 14, núm. 1, 2025.

DOMURATH, I.: "Digital Vulnerability as a Power Relation" en *The New Shapes of Digital Vulnerability in European Private Law* (eds. CREA, C. y DE FRANCESCHI, A.), Nomos, 2024.

FELIU ÁLVAREZ SOTOMAYOR, S.: "Ámbito territorial y aplicación del principio del control en origen en el Reglamento UE de servicios digitales", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, 2024.

GASCÓN MARCÉN, A.: "La diligencia debida en los Reglamentos de Servicios Digitales e Inteligencia Artificial" en *Empresa y derechos humanos: retos y tendencias normativas ante un complejo e inédito contexto geoestratégico* (Dir. JJ., ALVAREZ RUBIO), Aranzadi, 2025.

GASCÓN MARCÉN, A.: El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea, *Cuadernos de derecho transnacional*, vol. 13, n.º 2, 2021.

GENOVESI, S.; KAESLING, K. y ROBBINS, S. (ed.): *Recommender Systems: Legal and Ethical Issues*, Springer, 2023.

GOANTA, C., DE GREGORIO, G., SPANAKIS, J.: "Consumer Protection and Digital Vulnerability: Common and Diverging Paths", en *The New Shapes of Digital Vulnerability in European Private Law* (eds. CREA, C. y DE FRANCESCHI, A.), Nomos, 2024.

HELBERGER, H. y otros, *Digital Fairness for Consumers*, BEAUC, 2024.

HESS, B.: "Reforming the Brussels Ibis Regulation: Perspectives and Prospects", *MPILux Research Paper series*, 4, 10, 2021.

KÜHLING, J.: "Digital fairness in online retail", 2024.

LAPIEDRA ALCAMI, R.: "Hacia la transparencia y la equidad en el 'ranking' de resultados a la luz del Reglamento 2019/1150", en *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi Thomson Reuters, 2021.

LAPIEDRA ALCAMÍ, R.: "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad digital" en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, 2024.

LAPIEDRA ALCAMÍ, R.: "Hacia un entorno digital seguro para la infancia: el marco europeo y estatal de protección de los menores", en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

MADIEGA T.: "Digital sovereignty for Europe", *EPRS Ideas Paper Towards a more resilient EU*, 2020.

MATO PACÍN, M.N.: *Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros*, Agencia Estatal BOE, Colección Derecho Privado 29, Madrid, 2024.

NAMYSŁOWSKA, M.: "The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices", *Journal of Consumer Policy*, 2025.

NEUDERT, L.M. & MARCHAL, M.: *Polarisation and the use of technology in political campaigns and communication*, EPRS, 2019.

NIKIFOROV, L., *Digital Fairness Act: If and How*, Brussels Privacy Hub, 2024.

OECD, *Dark commercial patterns*, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, 2022.

PARISER, E.: *The filter bubble: What the internet is hiding from you*, Penguin Press, 2011.

PLA ALMENDROS, R., *La solución extrajudicial de disputas transfronterizas en el Reglamento de Servicios Digitales,* Colex, A Coruña, 2025.

REIG FABADO, I.: "Las VLOPS y los riesgos sistémicos en la DSA: algunos aspectos problemáticos", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. CASTELLÓ PASTOR, J.J.), Aranzadi, Cizur Menor, 2024.

REIG FABADO, I.: "Inteligencia Artificial y tutela jurídica de derecho digitales en la UE" en *Hacia una transición digital centrada en la persona: estudios jurídicos desde la perspectiva de la Unión Europea* (Coord. CASTELLÓ PASTOR, J.J.), Aranzadi, 2025.

TORNADA, J.: "How (Not) To deal with the Bubble Effect in Cyberspace: The Case of the EU and Digital Services Act", *Brook. J. Int´l L.*, vol. 49, 2024.

TRUJILLO CABRERA, C.: "Los nuevos cookie walls: 'consent or pay'. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023", *Revista de Derecho Civil*, vol. XI, núm. 2, 2024.

Capítulo 2

Hacia un entorno digital seguro para la infancia: el marco europeo y estatal de protección de los menores*

Rosa Lapiedra Alcamí
Prof.ª Titular de Derecho Internacional Privado
Universitat de València

SUMARIO: I. INTRODUCCIÓN. II. LA ESPECIAL VULNERABILIDAD DE LOS MENORES Y LA NECESIDAD DE PROTECCIÓN EN EL ENTORNO DIGITAL. 1. *Principales riesgos para los menores en la* red. III. MARCO NORMATIVO EUROPEO Y ESTATAL EN MATERIA DE PROTECCIÓN DE MENORES EN LA RED. 1. *Las medidas de protección de los menores en el entorno digital previstas en el Reglamento (UE) 2022/2065, de servicios digitales*. a) Prohibición de dirigir publicidad a menores basada en perfiles. 2. *Medidas de protección previstas en el Reglamento (UE) 2024/1689, de inteligencia artificial*. 3. *Medidas de protección previstas en el Reglamento (UE) 2023/2854, de datos*. 4. *Medidas de protección previstas en el Proyecto de Ley Orgánica para la protección de menores en entornos digitales*. IV. NUEVOS MECANISMOS DE VERIFICACIÓN DE LA EDAD PARA EL ACCESO DE LOS MENORES A LOS SERVICIOS DIGITALES: EL REGLAMENTO (UE) 2024/1183, DE IDENTIDAD DIGITAL. V. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

En las últimas décadas, hemos sido testigos de una revolución tecnológica que ha transformado prácticamente todos ámbitos de nuestra vida

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro la autora.

diaria, en especial, la forma en que nos comunicamos y relacionamos con los demás. En efecto, las nuevas tecnologías están omnipresentes y hacen nuestra vida mucho más fácil. Por ejemplo, basta pensar cuando recurrimos a los asistentes virtuales como *Siri* o *Alexa* para conocer las noticias más destacadas del día; cuando accedemos a aplicaciones en los *smartphones* para conocer la previsión del tiempo en cualquier lugar del mundo, o para que nos proporcione las indicaciones para llegar a un lugar concreto.

Si bien es cierto que todos los avances tecnológicos aportan numerosos beneficios, tanto desde la perspectiva personal como profesional. No debemos olvidar que, en el caso de los menores de edad, el acceso a las redes sociales y otros servicios digitales lleva aparejados numerosos riesgos por el hecho de tratarse de un colectivo especialmente vulnerable. De ahí que las nuevas tecnologías conllevan un potencial peligro si no se hace un uso correcto de las mismas. Esta situación se agrava todavía más, si cabe, con el auge de la Inteligencia Artificial, —en adelante, IA— que, unido a las redes sociales y el acceso incontrolado de los menores al espacio virtual, puede provocar graves problemas de salud tanto físicos, como mentales y emocionales. Por no hablar de dificultades de interacción social, aislamiento o problemas en el desarrollo cognitivo[1].

Actualmente, los menores utilizan a diario plataformas digitales como *youtube, twich, tik tok* e *Instagram,* no solo como vías de entretenimiento, sino también como mecanismos de socialización. El incremento de la actividad de los menores en la red ha generado una enorme preocupación tanto en el ámbito jurídico, como en el educativo y familiar. Ello es así por cuanto que la población infantil está expuesta a toda una serie de riesgos que inciden directamente en los derechos fundamentales de los menores, pudiendo poner en peligro, tanto su integridad física, como psíquica.

En este contexto, este trabajo de investigación tiene como objetivo, por un lado, analizar los principales riesgos que enfrentan los menores en el entorno digital, con especial atención al papel de las redes sociales. Y, por otro lado, examinar las medidas previstas en los principales instrumentos normativos que se han elaborado en el ámbito europeo y en el estatal con el objeto de mitigar todos estos peligros.

---

1. Exposición de motivos del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el BOCG, el 11 de abril de 2025, p. 2; MARTÍNEZ, G., GARMENDIA, M., GARITAONANDIA, C.: "La infancia y la adolescencia ante las tecnologías de la información y la comunicación (TIC): oportunidades, riesgos y daño", *Zer*, 2020, 25 (48), p. 357.

II. LA ESPECIAL VULNERABILIDAD DE LOS MENORES Y LA NECESIDAD DE PROTECCIÓN EN EL ENTORNO DIGITAL

La protección de los menores siempre ha sido una prioridad, tanto en el ámbito europeo como en el estatal. Es por ello que debería ser el criterio determinante para las plataformas a la hora de diseñar sus servicios digitales. Tal es así, que el interés superior del menor se configura como como un principio de orden público[2] y uno de los objetivos políticos más importantes de la Unión[3]. En efecto, constituye el eje central de toda la normativa europea, no solo en materia de Derecho de familia, sino también a la hora de regular el entorno digital por parte de la Unión Europea[4].

La Carta de los derechos fundamentales de la Unión Europea, —en adelante, CDFUE—[5] constituye el instrumento jurídico que recoge los derechos y libertades fundamentales de los ciudadanos europeos con el objeto de ofrecerles una protección integral. En consecuencia, los derechos allí recogidos resultan de obligado cumplimiento por parte de todos los operadores jurídicos. De entre todos los derechos enumerados en la Carta Magna, vamos a hacer referencia a los más pertinentes en relación con la protección de los menores en el entorno digital[6]. En primer lugar, el principio del "interés superior del menor"[7] —art. 24.2 CDFUE— En segundo lugar, el "derecho a la protección del menor" —art. 24.1 CDFUE—; En tercer lugar, el "derecho a la libertad de expresión" —art. 24.1 CDFUE—; Junto a este, el "derecho a no sufrir discriminación" —art. 21 CDFU—; el "derecho a la protección de los datos personales" —art. 8 CDFUE—; y, finalmente, el "derecho a un alto

2. Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Publicada en el Boletín Oficial del Congreso de los Diputados, Serie A: Proyectos de Ley, 11 de abril de 2025, núm. 52-1, pág. 3.
3. Considerando 71 del Reglamento (UE) 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) —RSD—.
4. Considerando 89 Reglamento (UE) 2022/2065 —RSD—: "Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben tener en cuenta el interés superior de los menores a la hora de adoptar medidas como adaptar el diseño de su servicio y su interfaz en línea, en especial cuando sus servicios se dirijan principalmente a menores o sean utilizados predominantemente por ellos".
5. https://www.boe.es/doue/2010/083/Z00389-00403.pdf
6. MORALEJO IMBERNON, N.: *Los derechos de los menores y las redes sociales*, Valencia, Tirant lo Blanch, 2023, p. 87 y ss.
7. MORENO PIZARRO, E., RIVERO HERNÁNDEZ, F.: *El interés superior del menor: Claves jurisprudenciales,* Ed. Reus, 2020, p. 28.

nivel de protección de los consumidores" —art. 38 CDFUE—[8], por cuanto que los menores también pueden ser consumidores.

Es evidente que la protección de todos estos derechos debe garantizarse, no solo en el entorno físico, sino también en el digital. Tal y como establece la Agencia Española de Protección de Datos, la protección en el entorno digital exige una visión global del interés superior del menor y de la protección de sus derechos fundamentales[9]. Es decir, un entorno digital seguro no puede limitarse a unos aspectos concretos como, por ejemplo, el acceso a contenido inadecuado o problemas de adicción a las redes. En consecuencia, todos los derechos que afectan a los menores no pueden ser considerados de forma aislada, sino que tienen que contemplarse de forma integral, sin establecer ninguna jerarquía o prioridad entre ellos[10].

1. PRINCIPALES RIESGOS PARA LOS MENORES EN LA *RED*

Hoy en día los menores se incorporan al mundo digital en edades cada vez más tempranas. Esta realidad impone un deber reforzado a los titulares de la patria potestad y a los poderes públicos de adoptar medidas adecuadas para proteger sus derechos en el entorno digital, en cuanto garantes del desarrollo integral del menor. Si bien, lo cierto es que esta circunstancia pone de manifiesto que son los padres los responsables últimos de proporcionar acceso a los menores a los dispositivos digitales en edades totalmente inapropiadas[11]. Y, no olvidemos que, los progenitores, en su condición de titulares de la patria potestad, tienen la obligación de proteger los derechos e intereses de sus hijos menores, ejerciendo las funciones inherentes a la patria potestad, conforme al principio del interés superior del menor[12]. Así como

8. *The Digital Services Act (DSA) explained, Measures to protect children and young people online*, accesible en https://op. europa.eu/en/publication-detail/-/publication/f3556a65-88ea-11ee-99ba-01aa75ed71a1
9. https://www.aepd.es/memorias/memoria-aepd-2024.pdf
10. Informe de la Agencia Española de Protección de Datos —AEPD—: "Internet seguro por defecto para la infancia y el papel de la verificación de la edad", https://www.aepd.es/guias/nota-tecnica-internet-seguro-por-defecto-para-la-infancia.pdf, publicado en octubre de 2024.
11. MORILLAS FERNÁNDEZ, M.: "Menores vulnerables y redes sociales: nuevos retos jurídicos en la protección ante el uso inadecuado: edad, educación y controles por defecto", *Revista Internacional de Doctrina y Jurisprudencia*, vol. 32, dic. 2024, p. 48. (47-70).
12. Así se desprende de los artículos 154 Cc español, art. 5 de la Ley Orgánica 1/1996, de Protección Jurídica del Menor, y del artículo 18 de la Convención de Naciones Unidas sobre los Derechos del Niño.

también, les corresponde a los padres dar buen ejemplo de cómo hacer un buen uso de la tecnología.

El hecho de introducirse en el entorno digital a edades tan tempranas conlleva un riesgo adicional. Ello es así porque, a medida que los niños van creciendo, empiezan a interactuar de manera autónoma e incluso con una cierta relajación en cuanto al control parental, pese a ser todavía menores de edad. Sin embargo, es precisamente a partir de ese momento cuando aumentan las curiosidades propias de la edad y aparecen los mayores peligros en la red[13].

Las personas nacidas a partir de los años 80 o 90 son denominadas "nativos digitales"[14] por el hecho de haber nacido en un entorno tecnológico perfectamente desarrollado. Es por ello por lo que, de forma innata, poseen grandes habilidades para manejarse con las Tecnologías de la Información y de la Comunicación, —en adelante, TIC— y las integran de forma natural en sus procesos de socialización, comunicación y aprendizaje, sin necesidad de adaptación previa. Esta condición los diferencia de generaciones anteriores, comúnmente denominadas "inmigrantes digitales"[15]. Estos últimos se han incorporado a estos entornos de manera progresiva y con mayores esfuerzos de adaptación.

Sin embargo, los menores, pese a disponer de todas estas habilidades naturales para manejarse con gran destreza en la tecnología, presentan importantes carencias que los expone a numerosos riesgos[16]. Por un lado, carecen de la madurez suficiente, debido a su corta edad, Y, por otro lado, pese a ese fácil manejo de las nuevas tecnologías, les falta una educación digital adecuada. En consecuencia, no son capaces ni de evitar las situaciones de riesgo a las que están expuestos, ni de prever las consecuencias de sus propios actos[17]. Esta circunstancia los convierte en especialmente vulnerables siendo víctimas muy fáciles. Es por ello por lo que algunos autores muy acertadamente los han calificado, más bien, de "huérfanos digitales"[18].

13. MORILLAS FERNÁNDEZ, M.: "Menores vulnerables…", cit., p. 50.
14. PALFREY, J., & GASSER, U.: *Born digital: Understanding the first generation of digital natives,* 2008, Basic Books/Hachette Book Group.
15. PRENSKY, M.: "Digital Natives, Digital Immigrants". On the Horizon, Vol. 9 No. 5, 2001.
16. ANDRADE, B., GUADIX, I., RIAL, A. Y SUÁREZ, F.: "Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades", Madrid, UNICEF, 2021, pp. 1-7.
17. CATALINA GARCÍA, B., LÓPEZ DE AYALA, M.C., GARCÍA JIMÉNEZ, A.: "Los riesgos de los adolescentes en internet: los menores como actores y víctimas de los peligros de Internet", *Revista Latina de Comunicación Social*, 2014, p. 463. (pp. 462-485); MORILLAS FERNÁNDEZ, M.: "Menores vulnerables…", cit., pp. 49 y 50.
18. MORILLAS FERNÁNDEZ, M.: "Menores vulnerables y…", cit., p. 49.

Veamos, algunas de las situaciones a las que se pueden enfrentar diariamente los menores en el entorno digital; usuarios adultos que falsean su edad para acercarse a menores en la red; se crean vídeos de contenido sexual con inteligencia artificial a partir de una foto real de un adolescente o se suplanta la identidad de una persona menor para acosarla. En este contexto, son muchos y de diversa índole los riesgos más frecuentes que pueden plantearse en el mundo digital. Riesgos a los que, en muchos casos, los adultos somos totalmente ajenos o ni siquiera somos capaces de percibir. Fenómenos como la violencia digital[19], ya sea a través del ciberacoso o el *grooming*[20], la exposición a contenidos nocivos[21], la falta de privacidad por recolección masiva de datos personales sin un consentimiento informado[22], la desinformación, la adicción digital[23] o la manipulación a través de la publicidad digital son algunos de los peligros de la red. Todos estos fenómenos se configuran como los principales retos a los que se enfrenta el derecho en su labor de garantizar una tutela efectiva de los derechos del menor. Estos riesgos preocupan a familias y autoridades, tal y como ponen de manifiesto las encuestas que muestran que más del 90 % de los ciudadanos en España y Europa considera muy peligroso el acceso indiscriminado de los menores a redes sociales[24].

Es por ello por lo que resulta del todo necesario fomentar y mejorar las competencias digitales, tanto en el ámbito familiar, como en el ámbito escolar con el objeto de garantizar a los menores una vida digital segura[25].

---

19. Para un estudio en profundidad sobre la cuestión *vid.* MARTÍNEZ, G., GARMENDIA, M., GARITAONANDIA, C.: "La infancia y la adolescencia ante las tecnologías de la información y la comunicación (TIC): oportunidades, riesgos y daño", *Zer*, 2020, 25 (48), pp. 351 y ss.
20. Hace referencia a la intimidación, amenazas o manipulación sexual en chats y redes.
21. El Informe EU Kids Online: elaborado por la Universidad del País Vasco cofinanciado por la UE denominado: "Actividades, mediación, oportunidades y riesgos online de los menores en la era de la convergencia mediática", ya advertía que más de un tercio de los niños ha visto material dañino estaban sometidos a este tipo de riesgos, disponible en https://bienestaryproteccioninfantil.es/informe-eu-kids-online-actividades-mediacion-oportunidades-y-riesgos-online-de-los-menores-en-la-era-de-la-convergencia-mediatica/
22. GARCÍA GARNICA, M.: "Datos personales y menores de edad", en *Protección de datos personales, Asociación de Profesores de Derecho civil,* Tirant Lo Blanch, 2020, p. 32.
23. *Vid.* el Capítulo V de la Memoria de la Fiscalía General del Estado 2024 está dedicado a "los menores y redes sociales", https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html.
24. Informe EU Kids Online: "Actividades, mediación, oportunidades y riesgos online de los menores en la era de la convergencia mediática".
25. NÚÑEZ GÓMEZ, P., ORTEGA MOHEDANO, F., LARRAÑAGA MARTINEZ, K.: "Hábitos de uso y consumo de pantallas inteligentes entre niños/as de 7 a 9 años en España", *Revista Mediterránea de Comunicación,* 12 (1), 2021, pp. 191-204.

Esta revolución tecnológica genera una enorme preocupación y, sobre todo, grandes retos sobre la privacidad, la seguridad de la información y el uso ético de los datos. En efecto, ¿cómo pueden los prestadores de servicios digitales encontrar un equilibrio entre ser eficientes, generar confianza entre los usuarios, proteger su privacidad y garantizar sus derechos fundamentales?

En este contexto resulta necesario garantizar la seguridad de los usuarios, especialmente los niños y los jóvenes, ante los peligros y riesgos en línea. Si bien, se debe encontrar un equilibrio entre el establecimiento de mecanismos de protección y control adecuados y eficaces, sin que ello suponga una vulneración del derecho a la intimidad de los adolescentes. El objetivo, sin duda debe ser aprovechar todas las ventajas que ofrece la innovación tecnológica, pero de manera responsable. Esto es, de forma ética protegiendo en todo momento los derechos fundamentales de los usuarios en la red. Es por ello por lo que, su desarrollo y aplicación deben ir acompañados de regulaciones y principios éticos que garanticen un uso apropiado. Un elemento clave, que sin duda influye de forma directa en un uso responsable de las nuevas tecnologías y redes sociales en los menores es el ejemplo que den los progenitores al respecto[26].

III. MARCO NORMATIVO EUROPEO Y ESTATAL EN MATERIA DE PROTECCIÓN DE MENORES EN LA RED

En este contexto, el Estado y la Unión Europea, conscientes de todos los riesgos que implica el entorno digital, juegan un papel fundamental a la hora de proteger a la sociedad y, en especial a los menores, del impacto negativo que puede tener un uso irresponsable de todas las posibilidades que ofrece el entorno digital[27]. La Unión Europea con el objeto de hacer frente a todos los riesgos inherentes al entorno digital —que afectan en mayor medida a los menores— ha elaborado en los últimos años un amplio marco regulador. Esta normativa pretende crear un entorno digital seguro y responsable que garantice el respeto de los derechos fundamentales de todos los usuarios de la red. Algunos de los principales instrumentos que ha elaborado son; por un lado, el Reglamento (UE) 2016/679 de Protección de Datos[28] —en

26. ANDRADE, B., GUADIX, I., RIAL, A. Y SUÁREZ, F.: Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades, Madrid, UNICEF, 2021, p. 5.
27. MENDEZ SUAREZ, M., SIMÓN MOYA, V. Y MUÑOZ DE PRAT, J.M.: (2023) Do current regulations prevent unethical AI practices? *Journal of Competitiveness*, 15(3), pp. 207-222, https://doi.org/10.7441/JOC.2023.03.11
28. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento

adelante, RGPD—. Por otro lado, el Reglamento (UE) 2022/2065 de Servicios Digitales[29], —en adelante, RSD—. Y, más recientemente, el Reglamento (UE) 2024/1689 de Inteligencia Artificial[30], —en adelante, RIA—, el Reglamento (UE) 2024/1183 sobre la Identidad Digital Europea[31] y el Reglamento (UE) 2023/2854 de Datos[32]. Junto a ello, la Comisión Europea adoptaba una nueva estrategia para Europa una Internet Mejor para los Niños (BIK+), con el fin de mejorar los servicios digitales adaptados a su edad y garantizar que todos los niños estén protegidos, empoderados y respetados en línea[33].

En el ámbito estatal también hay novedades legislativas recientes en esta materia: Proyecto de Ley Orgánica para la protección de menores en entornos digitales, —en adelante, LOPMED—[34] y la Ley general de comunicación audiovisual[35] y el Real Decreto 444/2024, de 30 de abril[36], —conocida, comúnmente, como la Ley de *influencers*—.

---

de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, —en adelante, RGPD—.

29. Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), —en adelante, RSD—, también denominado Ley de Servicios Digitales, —DSA— (en vigor desde 17 febrero 2024).
30. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Este Reglamento fue aprobado por el Parlamento Europeo el 13 de marzo de 2024 y por el Consejo de la UE el 21 de mayo de 2024. Entró en vigor el 1 de agosto de 2024. La aplicación de sus distintas disposiciones será progresiva. Aunque, con carácter general, el reglamento será aplicable a partir del 2 de agosto de 2026, Las prohibiciones en vigor desde el 2 de febrero 2025 y El Capítulo XII (Sanciones) serán aplicables a partir del 2 de agosto de 2025.
31. Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, conocido como el Reglamento de identidad digital.
32. Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).
33. https://digital-strategy.ec.europa.eu/es/policies/strategy-better-internet-kids
34. Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el Boletín Oficial de las Cortes Generales —BOCG— el 11 de abril de 2025, Serie A Proyectos de Ley, núm. 52-1.
35. La Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual entró en vigor el 9 de julio de 2022 tras su publicación en el Boletín Oficial del Estado. Esta ley trans-

Veamos, en primer lugar, cuáles son las medidas que imponen estos Reglamentos con el objeto de proteger a los menores en la red. De todos estos instrumentos normativos, si bien los mencionaremos todos, nos centraremos fundamentalmente en el RSD y en la LO de protección de menores —LOPMED— por ser los que prevén un mayor número de medidas específicas dirigidas a los menores. Y, a continuación, valoraremos en qué medida los prestadores de servicios digitales las están cumpliendo, teniendo en cuenta que la mayoría de estos instrumentos ya están en vigor y las empresas se enfrentan a grandes multas para el caso de incumplimiento.

1. LAS MEDIDAS DE PROTECCIÓN DE LOS MENORES EN EL ENTORNO DIGITAL PREVISTAS EN EL REGLAMENTO (UE) 2022/2065, DE SERVICIOS DIGITALES

La Unión Europea ha elaborado el Reglamento (UE) 2022/2065, de Servicios Digitales[37] que tiene por objeto "mejorar el funcionamiento del mercado interior y garantizar un entorno en línea seguro y transparente, y para ello es necesario establecer un conjunto claro, eficaz, predecible y equilibrado de obligaciones armonizadas de diligencia debida para los prestadores de servicios intermediarios"[38]. En concreto, el Reglamento RSD establece importantes prohibiciones y obligaciones específicas de transparencia dirigidas a todos los proveedores de servicios de intermediación en línea —art. 26 RSD—[39]. Junto a ello, el Reglamento impone, asimismo, obligaciones adi-

---

pone al ordenamiento jurídico español la Directiva (UE) 2018/1808, que modifica la Directiva de Servicios de Comunicación Audiovisual (Directiva 2010/13/UE). La Directiva 2018/1808 amplía su ámbito de aplicación a plataformas de intercambio de vídeos y servicios similares, con el objetivo de adaptar la normativa a la evolución del entorno digital.

36. Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual

37. Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), —en adelante, RSD—, también denominado Ley de Servicios Digitales, —DSA—.

38. Considerando 40 del Reglamento (UE) 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) —RSD—.

39. En relación con las medidas obligatorias en materia de información y transparencia a las plataformas en línea, véase CASTELLÓ PASTOR, JJ. "Interrelación del Reglamento de servicios digitales con el Reglamento *Platform to Business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en *Análisis del*

cionales cuando los usuarios son menores de edad, con el objeto de reforzar su protección por considerarse personas especialmente vulnerables.

En definitiva, el RSD elabora un conjunto de normas para proteger, por un lado, los derechos de los usuarios consagrados en la Carta de los derechos fundamentales de la Unión Europea. Y, por otro lado, trata de definir responsabilidades claras para los proveedores de servicios intermediarios y redes sociales[40]. Finalmente, pretende aumentar la transparencia en el entorno digital y hacer frente a los contenidos y productos ilícitos. Todo ello debe entenderse sin perjuicio de la aplicación de las disposiciones pertinentes del RGPD, en particular, las relativas a la necesidad de obtener el consentimiento del interesado para el tratamiento de los datos personales[41].

Las plataformas en línea deben garantizar que los derechos de los usuarios en general y el interés superior de los niños, en particular, constituya el eje central a la hora de diseñar sus servicios. Asimismo, los proveedores de servicios digitales deben adoptar un enfoque basado en el riesgo, llevar a cabo periódicamente evaluaciones de impacto y aplicar medidas de mitigación de cualquier riesgo potencial para los menores derivado de sus servicios[42].

Vamos a analizar las medidas concretas de protección de los menores en los espacios digitales que prevé el RSD. En este contexto, el art. 28 del RSD impone a los prestadores de los servicios de intermediación en línea una serie de medidas destinadas a proteger a los menores en el entorno digital. En realidad, el art. 28 RSD establece un marco de actuación protocolizado destinado a proteger a los menores en la red. En concreto, prevé obligaciones

---

Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea, en CASTELLÓ PASTOR, J.J. (Dir.), Aranzadi (Thomson Reuters), 2024, pp. 361 y ss.; SENFTLEBEN, M.: "trademark law, al-driven behavioural advertising and the Digital Services Act — towards source and parameter transparency for consumers, Brand owners and competitors", chapter 16, *Collection Law* 2022, https://doi.org/10.4337/9781800881907.00023.

40. Así se dispone expresamente en el art. 1.1 del Reglamento RSD https://www.europarl.europa.eu/charter/pdf/text_es.pdf.

41. *Vid*. el Considerando 68 del Reglamento (UE) 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) —RSD—.

42. Considerandos 80, 81 y 89 del Reglamento (UE) 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) —RSD—.

de carácter general en el apartado 1 del art. 28 RSD y, junto a ello establece algunas prohibiciones en el art. 28.2.RSD.

Por lo que a las obligaciones se refiere, el art. 28.1 del RSD exige, por un lado, a los prestadores de plataformas en línea establecer "medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en su servicio" —art. 28.1 RSD—[43]. Sin embargo, se trata de una norma muy general que no concreta ninguna acción al respecto, por lo que se podría decir que el precepto está vacío de contenido. De ahí que resulte más bien un protocolo de protección digital. Es por ello que resulta del todo necesario fijar pautas concretas que sean efectivas y comunes a todos los prestadores de servicios digitales.

Con el objeto de dar cumplimiento a este protocolo de actuación, el art. 28.4 RSD[44] se contempla la posibilidad de que la Comisión elabore unas "Directrices" para guiar a los prestadores de plataformas en línea acerca de cómo dar cumplimiento a estas medidas adecuadas y proporcionadas. De ahí que será determinante su elaboración a efectos de concretar qué reglas deberán adoptar los servicios de intermediación en línea para proteger de forma efectiva a los menores frente a los peligros de la red. Qué duda cabe que la mejor forma de facilitar el cumplimiento de las obligaciones impuestas por el Reglamento es estableciendo una guía con una lista concreta de medidas que deben adoptar los proveedores de los servicios de información.

La elaboración de estas Directrices se estima clave para asesorar a las plataformas en línea acerca de cómo deben aplicar altos niveles de privacidad, seguridad y protección para los menores en línea, tal como exige el Reglamento de Servicios Digitales en el art. 28.1. Es por ello que, a continuación, vamos a determinar qué órgano es el encargado de elaborar estas directrices y cuál ha sido el proceso de elaboración que se ha llevado a cabo.

El Consejo Europeo de Servicios Digitales ha creado ocho grupos de trabajo, cada uno dedicado a un aspecto específico del RSD. En concreto, el Grupo de Trabajo 6 del Comité Europeo de Servicios Digitales[45] se dedica a

43. Art. 28.2 DSA: Protección de los menores en línea: "1. Los prestadores de plataformas en línea accesibles a los menores establecerán medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en su servicio".

44. Art. 28.4 RSD: Protección de los menores en línea: (…) "4. La Comisión, previa consulta a la Junta, podrá proporcionar directrices para guiar a los prestadores de plataformas en línea en la aplicación del apartado 1".

45. https://digital-strategy.ec.europa.eu/en/library/working-group-6-european-board-digital-services-protection-minors

la protección de menores. Este grupo está presidido por la Comisión Europea y cuenta con la participación de representantes de los Estados miembros que ya han celebrado reuniones desde septiembre de 2024 para avanzar en la elaboración de estas directrices.

El pasado 31 julio de 2024 se abrió un período de dos meses, hasta el 30 de septiembre de 2024 con el objeto de recabar toda la información necesaria procedente de todas las partes interesadas y grupos de interés, incluyendo informes científicos y estudios de investigación[46]. La Comisión estima clave todas estas aportaciones para elaborar las directrices. De entre las cuestiones que estas directrices incluirán destacan: buenas prácticas y medidas de mitigación de los riesgos[47] a los que pueden enfrentarse los menores en la red. Toda la información recabada se estima clave, asimismo, para concretar el alcance de las Directrices, así como el enfoque de las mismas[48]. A continuación, el 4 de octubre de 2024, se celebró un taller de expertos que reunió a más de 140 especialistas de diferentes ámbitos, como coordinadores de servicios digitales, autoridades nacionales, organizaciones civiles, plataformas en línea, académicos y embajadores juveniles. Durante este evento, se discutieron riesgos específicos que enfrentan los menores en línea y se compartieron buenas prácticas y recomendaciones para abordarlos.

Con toda la información recabada, el Grupo de Trabajo 6 del Comité Europeo de Servicios Digitales ha elaborado la versión final de las Directrices previstas en el artículo 28.4 del Reglamento de Servicios Digitales en mayo de 2025[49]. Finalmente, la Comisión europea publicaba el 13 de mayo de 2025 un proyecto de directrices sobre la protección de los menores en línea[50]. A continuación, se abría un período de consulta pública desde el 13

46. https://digital-strategy.ec.europa.eu/es/news/commission-launches-call-evidence-guidelines-protection-minors-online-under-digital-services-act
47. REIG FABADO, I.: "Las VLOPs y los riesgos sistémicos en la DSA: algunos aspectos problemáticos", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, en CASTELLÓ PASTOR, J.J. (Dir.), Aranzadi (Thomson Reuters), 2024, pp. 292 y ss; CASTELLÓ PASTOR, JJ., Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea, *Cuadernos de derecho transnacional*, Vol. 17, N.º 1, 2025, págs. 308-328.
48. https://digital-strategy.ec.europa.eu/en/library/working-group-6-european-board-digital-services-protection-minors
49. https://ec.europa.eu/eusurvey/runner/DSA_PoM_guidelines
50. https://ec.europa.eu/eusurvey/runner/DSA_PoM_guidelines. Para un análisis de estas medidas vid: DE MIGUEL ASENSIO, P. : "Protección de menores en línea (I): Directrices relativas al artículo 28(4) del Reglamento de Servicios Digitales", publicado

de mayo hasta el 10 de junio de 2025[51]. Una vez finalizado este periodo, las Directrices fueron publicadas oficialmente el pasado 10 de octubre de 2025 en el DOUE[52].

En efecto, finalmente, la versión definitiva de las "directrices" ha sido publicada oficialmente en el DOUE el pasado 10 de octubre de 2025[53] con el objeto de clarificar y concretar a los prestadores las medidas a adoptar. En líneas generales, las principales medidas que establecen son las siguientes: por un lado, las plataformas, por defecto, deben estar diseñadas para proteger a los menores por lo que las interfaces deberán estar adaptadas a su edad. Por otro, deben implementar controles parentales eficaces. Además, queda prohibida la publicidad basada en perfiles para menores. Junto a ello, las plataformas deben proporcionar información clara y comprensible sobre los parámetros principales utilizados en sus sistemas de recomendación, así como ofrecer opciones para que los menores puedan modificar o influir en dichos parámetros. Se hace hincapié en la necesidad de implementar mecanismos de verificación de edad en línea con las iniciativas de la UE —la cartera digital europea— para mejorar la protección de los menores en línea. Por supuesto, las cuentas deben ser privadas, por defecto, para los menores reduciendo los diseños adictivos especialmente en plataformas utilizadas por menores. Las plataformas deben participar en la elaboración de códigos de conducta y compartir buenas prácticas. Y, finalmente, las plataformas deben designar responsables que garanticen el cumplimiento y la eficacia de estas medidas[54].

Una vez aprobadas las "directrices" sobre la protección de los menores resultarán de aplicación a todas las plataformas en línea. Y, todo ello, con independencia de que vayan o no dirigidas específicamente a menores. Ello es así por cuanto que a fecha de hoy no se dispone de mecanismos fiables y eficaces de verificación de la edad. Si bien es cierto que se haya en proceso muy avanzado la creación de la cartera de identidad digital europea, como

---

el 31 de mayo de 2025 en: https://pedrodemiguelasensio.blogspot.com/2025/05/proteccion-de-menores-en-linea-i.html

51. Comunicación de la Comisión de 13 de mayo de 2025 donde se publica la versión final de las Directrices. El texto final está abierto a consulta pública hasta el 10 de junio de 2025: "Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065". https://ec.europa.eu/eusurvey/runner/DSA_PoM_guidelines
52. Diario Oficial de la Unión Europea DOUE, Serie C-2025/5519.
53. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:C_202505519
54. https://digital-strategy.ec.europa.eu/es/news/commission-launches-call-evidence-guidelines-protection-minors-online-under-digital-services-act

veremos más adelante. De ahí que actualmente cualquier menor, si falsea sus datos al registrase, puede tener acceso a todas las plataformas, al margen de que sea adecuada o no a su edad con el peligro que entraña. No en vano, la Comisión y los Estados miembros están centrando los esfuerzos en la cuestión que deviene clave y es, precisamente, cómo establecer mecanismos fiables de verificación de la edad. que ha dado como fruto, tal y como veremos, el Reglamento (UE) 2024/1183, de identidad digital.

El contenido de las directrices termina de conocerse, sin embargo, al estar ya en vigor este Reglamento algunas de las plataformas más utilizadas entre los adolescentes ya han implementado algunas medidas para dar cumplimiento a las obligaciones de protección de los menores y evitar así las elevadas sanciones que les puede imponer la Unión Europea.

Esto es precisamente lo que ha ocurrido con Instagram que desde comienzos de 2025 ha empezado a imponer las "Cuentas para adolescentes" —*Teen Accounts*— en España y en Europa. De manera que los usuarios entre 14 y 17 años dispondrán de funciones de protección integradas. En concreto, las cuentas de los menores serán privadas por defecto y con una configuración especial que tiene como objetivo proteger a los adolescentes, limitando cuestiones como quién puede ponerse en contacto con ellos, mostrando contenido adecuado para su edad y ayudándolos a administrar su tiempo en la plataforma. Estos parámetros de protección se activarán automáticamente de la siguiente manera: el adolescente recibirá una notificación en su *smartphone* informando sobre la conversión de las Cuentas en la de adolescente y en un plazo de siete días, su cuenta adoptará las medidas de protección mencionadas. Ahora bien, no olvidemos que estas funciones de protección únicamente se activarán si el menor al registrarse ha introducido su edad real, de no ser así, estos mecanismos de salvaguarda no se activarán. De ahí la importancia de la supervisión de los padres para verificar que los datos introducidos son los correctos.

a) Prohibición de dirigir publicidad a menores basada en perfiles

Otro de los temas controvertidos en relación con los menores refiere a la publicidad digital presentada a través de los espacios digitales. Ello es así por cuanto que, actualmente, los niños y adolescentes con acceso a las redes sociales se enfrentan a diario a mensajes informativos y publicitarios que ponen en grave riesgo su integridad física y psíquica.

En efecto, los menores están expuestos a diario a mensajes persuasivos de carácter comercial y a anuncios que proponen un modelo para ser acep-

tado socialmente. El problema estriba en que en la inmensa mayoría de las ocasiones los mensajes que reciben son publicidad, pero los menores no lo perciben como tal[55]. Tal es así que, una de las conclusiones principales del estudio realizado por UNIR en colaboración con Mapfre revela que casi la mitad de los niños entre 10 y 14 años no son capaces de identificar como publicidad ese tipo de mensajes en las redes sociales[56].

El enorme peligro que supone para los menores estriba en que la publicidad digital ejerce una enorme influencia sobre los jóvenes, no sólo porque condiciona sus hábitos de consumo y sus decisiones de compra, sino porque condiciona sus estilos de vida, sus actitudes, su sistema de creencias y valores sociales. De ahí que obviamente la vulnerabilidad y permeabilidad de los menores todavía es mucho mayor y la publicidad dirigida los deja completamente indefensos. A título de ejemplo, actualmente, según las estadísticas, cada vez hay más menores adictos al juego *online*, ya que habitualmente se ven expuestos a este tipo de publicidad. Junto a ello, tal como refleja el estudio de Fundación Mapfre y UNIR, el 46% de los menores se decide por una marca cuando la ha destacado un *influencer*[57]. Es más, hoy en día la aparición de los *influencers* virtuales ha supuesto una transformación de la industria publicitaria y se ha convertido en una herramienta estratégica para las grandes marcas por su enorme capacidad para conectar con los adolescentes[58]. Esta es precisamente la razón por la que se ha elaborado recientemente la ya conocida como Ley de *influencers*[59]. Y, es evidente que,

---

55. FEIJOO, B., SÁDABA, C.: When Ads Become Invisible: Minors' Advertising Literacy While Using Mobile Phones, *Media and Communication*, 2022, Vol. 10, Issue 1, p. 340, https://doi.org/10.17645/mac.v10i1.4720; FEIJOO, B., NÚÑEZ GÓMEZ, P., ÁLVAREZ FLORES, E.P.: "La alfabetización publicitaria de niños y adolescentes ante los nuevos formatos digitales", Revista Científica de Comunicación Aplicada, núm. 15(1), 2025, pp. 14 y 15.
56. https://www.fundacionmapfre.org/blog/la-responsabilidad-de-los-influencers-en-la-salud-de-sus-seguidores/
57. FERRER-LÓPEZ, M.: "Neuromarketing y la medición del efecto de la publicidad de influencers en adolescentes", *Revista Mediterránea de la Comunicación/Mediterranean Journal of Communication*, 11(2), pp. 244 y ss. https://www.doi.org/10.14198/MEDCOM2020.11.2.11; vid., asimismo, https://www.fundacionmapfre.org/blog/la-responsabilidad-de-los-influencers-en-la-salud-de-sus-seguidores/
58. Para más un análisis acerca de los influencers virtuales *vid.* RODRIGO MARTÍN, L., RODRIGO MARTÍN, I., MUÑOZ SASTRE, D.: "Los influencers virtuales como herramienta publicitaria en la promoción de marcas y productos. Estudio de la actividad comercial de Lil Miquela", *Revista Latina de Comunicación Social,* núm. 79, 2021, p. 89-90.
59. Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, de 7 de

los *influencers* deberán cumplir, asimismo, con la normativa de protección de menores. Por ejemplo, queda prohibida la publicidad de productos que vayan dirigidos a menores tales como productos nocivos para la salud como el tabaco, alcohol, cigarrillos electrónicos, … etc.

En este contexto, el art. 28.2 RSD[60] prohíbe a los prestadores de plataformas en línea la presentación de anuncios en su interfaz basados en la elaboración de perfiles[61] cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor. De ello se deduce que, si la plataforma desconoce que el usuario es un menor de edad y le ofrece publicidad inapropiada a su edad, no vulnera el art. 28.3[62] del Reglamento de Servicios Digitales. Sin embargo, si ya disponen de esa información, deben aplicar medidas de protección específicas para menores que exige el Reglamento de Servicios Digitales. El problema estriba en como los prestadores van a tener la certeza de que el destinatario del servicio digital es un menor ante la ausencia de sistemas fiables de verificación de la edad.

Debe tenerse en cuenta que hoy en día la mayoría de los menores mienten sobre su edad al registrarse, de lo contrario muchos adolescentes no tendrían acceso a las redes sociales. En consecuencia, reciben constantemente publicidad dirigida personalizada en muchos casos inapropiada para su edad, con el enorme poder de manipulación que ello implica. De ahí la imperiosa

---

julio, General de Comunicación Audiovisual —conocida comúnmente como la "Ley de *influencers*"—.

60. Art. 28.2 DSA: Protección de los menores en línea: (…) 2. Los prestadores de plataformas en línea no presentarán anuncios en su interfaz basados en la elaboración de perfiles, tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679, mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor.

61. Tal y como se define "elaboración de perfiles" en el art. 4.4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Se entiende por elaboración de perfiles "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

62. Art. 28 DSA: Protección de los menores en línea: (…) "3. El cumplimiento de las obligaciones establecidas en el presente artículo no obligará a los prestadores de plataformas en línea a tratar datos personales adicionales a fin de evaluar si el destinatario del servicio es un menor".

necesidad de los padres de supervisar los datos introducidos por sus hijos menores cuando se registran en las redes sociales, porque eso va a determinar el tipo de anuncios que reciben. Junto a ello, les corresponde, asimismo, vigilar su actividad en la red para garantizar un uso correcto de la misma y evitar graves perjuicios para su salud física y psíquica.

El artículo 28.3[63] del Reglamento de Servicios Digitales establece que las plataformas en línea no están obligadas a recopilar más datos personales adicionales. Tampoco, deben realizar procesos invasivos de averiguación de información adicional de los que ya disponen, con el objeto de determinar si un usuario es menor de edad[64]. La Unión Europea pretende con esta medida proteger la privacidad y limitar la recogida de datos personales.

En estas circunstancias, las empresas que ofrecen servicios digitales podrán fácilmente eludir la prohibición de dirigir publicidad a menores. Y, ello por dos razones: por un lado, por la inexistencia de mecanismos eficaces de verificación de la edad. Y, por otro, unido a que los menores introducen datos erróneos acerca de su edad al registrarse. En efecto, como se ha visto, solo está prohibido si se tiene la certeza de que el destinatario es un menor, a efectos de activar la protección prevista en el art. 28.2 RSD. De ahí que se pone de nuevo de manifiesto la imperiosa necesidad de implementar mecanismos fiables de verificación de la edad y que salvaguarden la privacidad.

Vamos a valorar el impacto que está teniendo en la práctica este art. 28.3 del RSD en plataformas como *Instagram* o *TikTok* que son las plataformas estrella entre los adolescentes. Cuando un usuario se crea una cuenta en alguna de estas dos redes sociales, si declara ser menor de edad, la plataforma está obligada a activar las medidas de protección impuestas por el RSD para proteger a los menores. Estas medidas son las siguientes: a) Restringir o prohibir la publicidad personalizada, b) ocultar contenidos potencialmente nocivos, c) incorporar herramientas de control parental y d) establecer configuraciones de privacidad más estrictas por defecto. Por el contrario, si el usuario al registrarse miente acerca de la edad y declara que es mayor de 18 años —cuando en realidad tiene 14—, esta plataforma no tiene que implementar verificación obligatoria de edad

63. Art. 28 DSA: Protección de los menores en línea (…). "3. El cumplimiento de las obligaciones establecidas en el presente artículo no obligará a los prestadores de plataformas en línea a tratar datos personales adicionales a fin de evaluar si el destinatario del servicio es un menor".

64. *Vid.* arts. 28. 2 y 3 Reglamento (UE) 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) —RSD—.

(como pedir DNI, escaneo facial, etc). No se les exige investigar activamente para confirmar la edad del usuario. De ahí el importante rol de los padres, como se ha visto.

La cuestión radica para las plataformas en como compatibilizar el principio de minimización de datos[65] del RGPD con la seguridad razonable de que el destinatario del servicio es un menor. Sobre todo, cuando estemos ante servicios que, en teoría no van dirigidos a menores, pero en la práctica la mayor parte de usuarios son menores de edad, por cuanto que falsean sus datos al darse de alta en las redes sociales. Según el principio de minimización de datos[66], las plataformas solo pueden recabar aquellos datos mínimos necesarios para cumplir con la finalidad prevista.

En consecuencia, se genera una tensión entre la necesaria protección de los menores y el respeto a la privacidad que pone en riesgo la efectiva protección de los menores[67]. Esto es, la Unión Europea trata de proteger a los menores sin obligar a las plataformas a recolectar más datos. De este modo, los menores quedan totalmente desprotegidos, ya que la inmensa mayoría miente acerca de su edad el registrase.

Entendemos en este caso que, dado que la edad del usuario deviene clave para la correcta prestación del servicio digital, debería ser requisito imprescindible solicitar la edad de los usuarios al registrarse y recurrir a los mecanismos fiables de verificación de la edad y que salvaguardan la privacidad. En teoría, solo así se podría tener la certeza que se exige en el RGPD. Y, en consecuencia, se podrían adoptar las medidas de protección necesarias en materia de publicidad digital cuando se tratara de menores, esto es, dirigir anuncios acordes a la edad del usuario. Sin embargo, en la práctica el problema persiste puesto que los menores en la mayoría de los casos no introducen los datos correctos sobre su edad, por lo que resulta imposible tener certeza de la edad del usuario. De ahí que debería ser responsabilidad de los padres supervisar las acciones de sus hijos.

65. El art. 5.1.c) RGPD los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

66. A tenor de lo dispuesto en el art. 5.1.c) del Reglamento de Protección de Datos, los datos recabados deberán ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". El principal objetivo del "principio de minimización de datos" consiste en que las entidades u organizaciones no recaben, traten y almacenen más datos personales de los necesarios y durante un período de tiempo indefinido o demasiado largo, especialmente por los riesgos que esto puede suponer para los derechos y libertades de los interesados.

67. HERRERA DE LAS ERAS, R., PAÑOS PÉREZ, A.: *La privacidad de los menores en las redes sociales. Especial consideración al fenómeno influencer*, Atelier, 2022, pp. 52 y ss.

Esto pone de manifiesto la falta de diligencia por parte de las plataformas, así como, la ineficacia de los controles relativos al acceso a este tipo de plataformas por personas que no superan la edad exigida para ello[68]. Debe tenerse en cuenta que, por ejemplo, *Instagram* en España exige una edad mínima de 14 años y están introduciendo nuevos mecanismos de verificación de la edad. En efecto, y con el objeto de adecuarse a la normativa europea, *Instagram*, que constituye una de las plataformas estrella entre los adolescentes, comienza a expandir en algunos países[69] un nuevo mecanismo de verificación de la edad con el objeto de poder ofrecer contenido apropiado a la edad del usuario. Estos nuevos mecanismos de verificación de la edad consisten, bien en aportar un documento de identificación, por ejemplo, el DNI; pedir a amigos en común que verifiquen su edad o a través de un video-*selfie*[70]. En este último caso, *Instagram* se ha asociado con Yoti, una empresa especializada en métodos de IA para verificar la edad preservando en todo momento la privacidad por cuanto que las fotos son eliminadas automáticamente. A través de esta tecnología, y a partir de los rasgos faciales, es capaz de identificar la edad del usuario, pero no es capaz de reconocer su identidad, precisamente con el objeto de preservar la privacidad de los menores en todo momento.

Junto a ello, es de señalar que, el acceso de los menores a plataformas como *Instagram* o *Tik tok*, requieren de un previo registro lo que les obliga a introducir datos personales y unas condiciones generales que deben aceptar. Es por ello por lo que, los prestadores de servicios intermediarios que estén dirigidos principalmente a menores deben realizar un esfuerzo especial para que la explicación de sus condiciones generales pueda ser comprendida con facilidad por los menores —art. 14.3 RSD—[71]. La clave radica en cuando

68. DE MIGUEL ASENSIO, P. : "Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales", *La ley Unión Europea*, núm. 109, dic. 2022, p. 35.

69. México, Canadá, Corea del Sur, Australia, Japón y más países de Europa. Nuestro plan es que las herramientas de verificación de la edad estén disponibles en aún más países de todo el mundo en los próximos meses.

70. https://about.instagram.com/es-la/blog/announcements/new-ways-to-verify-age-on-instagram

71. El art. 14 RSD dedicado a establecer las condiciones generales de uso de los servicios de intermediación en línea establece en su apartado 3: "Cuando un servicio intermediario esté dirigido principalmente a menores o sea utilizado predominantemente por ellos, el prestador de dicho servicio intermediario explicará las condiciones y cualesquiera restricciones del uso del servicio de manera que los menores lo puedan comprender". *Vid.*, asimismo, el Considerando 46 del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de

debemos entender que el prestador del servicio ha hecho un esfuerzo razonable para verificar la validez del consentimiento prestado por un menor. Lo cierto es que las plataformas se limitan a incorporar un desplegable donde deben añadir su fecha de nacimiento, basta con cambiarla para poder tener un acceso completo a sus servicios[72].

Asimismo, como complemento al art. 28 RSD resulta necesario determinar cuándo se considera lícito el tratamiento de los datos personales de los menores de conformidad con lo dispuesto en el art. 8.1 RGPD. En este sentido, se entenderá que el menor ha prestado su consentimiento —directo, expreso e informado[73]— de forma lícita, en relación con los datos que manejan las plataformas, cuando tenga como mínimo 16 años y el consentimiento sea directo, expreso e informado. Si el niño es menor de 16 años, el tratamiento solo se considerará lícito si el consentimiento ha sido prestado por el titular de la patria potestad[74]. En este caso, la carga de la prueba recae sobre el responsable del tratamiento de los datos quien deberá verificar que el consentimiento fue autorizado por el titular de la patria potestad[75]. La edad mínima fijada por el legislador europeo es flexible. De ahí que nada impide que cada Estado miembro establezca una edad inferior a tal efecto, si bien el mínimo se fija en 13 años[76]. Esto es precisamente lo que ha ocurrido en España con ocasión de la nueva Ley Orgánica de Protección de menores en el entorno digital que ha elevado la edad de 14 a 16 para prestar su consentimiento para el tratamiento de datos.

---

servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

72. MORALEJO IMBERNON, N.: *Los Derechos de los menores y las redes sociales*, Tirant lo Blanch, Valencia, 2023, p. 3.
73. SERRANO-MAÍLLO, I.: "Menores y contenidos digitales. Derechos y obligaciones", *Revista Mediterránea de Comunicación,* vol. 13 (1), p. 107-122, p. 112.
74. *Vid.* el art. 8.1 RGPD: "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó".
75. *Vid*. el art. 8.2 RGPD: "El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible".
76. *Vid.* el Art. 8.1.1 *in fine* RGPD: "Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años".

2. MEDIDAS DE PROTECCIÓN PREVISTAS EN EL REGLAMENTO (UE) 2024/1689, DE INTELIGENCIA ARTIFICIAL

El Reglamento (UE) 2024/1689 de Inteligencia artificial[77], —en adelante, Reglamento IA—, está en vigor desde el 1 de agosto de 2024. Este instrumento establece un marco jurídico pionero para garantizar que los sistemas de IA desarrollados y utilizados en la Unión Europea sean seguros, éticos y respetuosos con los derechos fundamentales. Si bien es cierto que este Reglamento no regula expresamente la protección de los menores, sí que contempla algunas medidas importantes que indirectamente van a proteger a los menores en el entorno digital. En concreto, tal y como dispone el art. 5.1 queda prohibida la utilización de sistemas de IA en el mercado que permitan, tanto la explotación de vulnerabilidades de las personas, como la edad o la discapacidad así como el uso de técnicas subliminales, deliberadamente manipulativas o engañosas para alterar de manera sustancial el comportamiento de personas —art. 5.1 a) y b)—[78]. Estas disposiciones buscan garantizar un entorno digital seguro para todos los usuarios y, en especial, para los menores, protegiéndolos de posibles riesgos asociados al uso de tecnologías de IA.

Además, el Reglamento exige que los sistemas de IA de alto riesgo, que puedan afectar a los derechos fundamentales, estén sujetos a evaluaciones de impacto y cumplan con requisitos estrictos de transparencia y supervisión.

3. MEDIDAS DE PROTECCIÓN PREVISTAS EN EL REGLAMENTO (UE) 2023/2854, DE DATOS

El Reglamento (UE) 2023/2854, también conocido como el Reglamento de Datos[79] tampoco incluye disposiciones específicas orientadas exclusiva-

77. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).
78. Art. 5 Reglamento (UE) 2024/1689 sobre Inteligencia Artificial.
79. El Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) fue adoptado el 13 de diciembre de 2023 y publicado en el *Diario Oficial de la Unión Europea* el 22 de diciembre de 2023. Entró en vigor el 11 de enero de 2024. No obstante, su aplicación efectiva está prevista para el 12 de septiembre de 2025, fecha a partir de la cual sus disposiciones serán obligatorias para los Estados miembros y los operadores económicos. Si bien, algunas disposiciones que se implementarán en fechas posteriores.

mente a la protección de los menores en el entorno digital. Ello es así por cuanto su objetivo principal es regular el uso de los datos generados en la red. No obstante, sí incorpora principios generales que pueden inciden indirectamente en la protección de los menores en la red.

Por un lado, el Reglamento de datos promueve que los usuarios tengan mayor control y conocimiento sobre cómo se utilizan sus datos, lo cual es fundamental para proteger la privacidad de los menores. Por otro lado, se establecen restricciones contra cláusulas que impongan condiciones desleales, lo que puede evitar prácticas que perjudiquen a usuarios vulnerables, incluidos los menores. Y, finalmente, los proveedores deben garantizar que el acceso y uso de los datos se realice de manera justa y equitativa, lo que puede contribuir a un entorno digital más seguro.

En definitiva, aunque el Reglamento (UE) 2023/2854 de datos no aborda directamente la protección de los menores en el entorno digital, sus principios generales contribuyen a un marco más seguro y equitativo que, junto con otras normativas específicas, fortalecen la protección de los menores en el ámbito digital.

4. MEDIDAS DE PROTECCIÓN PREVISTAS EN EL PROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE MENORES EN ENTORNOS DIGITALES

La nueva Ley Orgánica para la protección de menores en entornos digitales[80] cuya entrada en vigor se prevé en breve introduce el marco normativo necesario para dar cumplimiento a los compromisos adquiridos por España, en materia de derechos de las personas menores de edad, ante la creciente importancia de los entornos digitales en el desarrollo de la sociedad.

El Consejo de Ministros de España aprobaba el pasado 25 de marzo de 2025 el Proyecto de Ley Orgánica para la protección de menores en entornos digitales. A partir de ese momento, el proyecto era remitido al Congreso de los Diputados para iniciar su tramitación parlamentaria. El Proyecto de Ley fue publicado el 11 de abril en el Boletín Oficial de las Cortes Generales —BOCG—, estableciendo un plazo de enmiendas que finalizaba el día 5 de mayo de 2025[81]. Finalizado este plazo, la mesa del Congreso se reunió

80. Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el Boletín Oficial de las Cortes Generales —BOCG— el 11 de abril de 2025, Serie A Proyectos de Ley, núm. 52-1.

81. El día 8 de abril de 2025 se reunía la mesa de la Cámara del Congreso y se acordaba encomendar el Dictamen, conforme al artículo 109 del Reglamento, a la Comisión

el 6 de mayo de 2025 y acordaba tramitar el proyecto por el procedimiento de urgencia[82] lo que implica que los plazos para su debate y aprobación se acortan, con el objetivo de que la Ley entre en vigor lo antes posible. El pleno del Congreso de los Diputados aprobaba el pasado 10 de septiembre de 2025 la tramitación del proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. A continuación, será remitida al Senado para continuar con su tramitación. De aprobarse esta Ley, España se convertiría en un país europeo pionero en esta materia.

En efecto, este nuevo Proyecto de Ley Orgánica de protección digital a menores consagra, por primera vez en España, los derechos de los menores en los entornos digitales. El principal objetivo de esta Ley es ofrecer espacios virtuales seguros para los adolescentes. A tal fin, prevé medidas para garantizar una completa protección de los derechos y libertades fundamentales de los menores. Asimismo, pretende asegurar un correcto desarrollo de su personalidad, a la vez que se fomenta un uso adecuado, respetuoso y responsable de las nuevas tecnologías[83]. Las medidas que se recogen en el Proyecto de Ley se desarrollan desde una perspectiva amplia y multidisciplinar con el objeto de conseguir una protección integral de los menores de edad en el mundo digital. Muy acertadamente, la Ley aborda los problemas desde una perspectiva preventiva, con el fin de ofrecer a través de los canales adecuados herramientas accesibles que permitan anticiparse al desarrollo de problemas más graves[84].

---

de Justicia. Asimismo, publicaba el Proyecto de Ley el 11 de abril en el Boletín Oficial de las Cortes Generales, estableciendo plazo de enmiendas, por un período de quince días hábiles, que finalizaba el día 5 de mayo de 2025. Y en ejecución de dicho acuerdo se ordena la publicación de conformidad con el artículo 97 del Reglamento de la Cámara.

82. La Mesa de la Cámara reunida el pasado 6 de mayo de 2025 acuerda solicitar la tramitación del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales por el procedimiento de urgencia, en los términos de lo dispuesto en el artículo 93.2 del Reglamento. Asimismo, acuerdan comunicar este acuerdo al Gobierno y a la Comisión de Justicia y publicarlo en el Boletín Oficial de las Cortes Generales. En ejecución de dicho acuerdo, se ordena la publicación de conformidad con el artículo 97 del Reglamento de la Cámara. Publicado en el BOCG el 9 de mayo de 2025, Serie A: Proyectos de Ley, núm. 52-2, p. 1.
83. Exposición de motivos del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el Boletín Oficial de las Cortes Generales —BOCG— el 11 de abril de 2025, Serie A Proyectos de Ley, núm. 52-1, p. 5 y art. 3 b).
84. Exposición de motivos del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el Boletín Oficial de las Cortes Generales —BOCG— el 11 de abril de 2025, Serie A Proyectos de Ley, núm. 52-1, p. 5.

El Proyecto de Ley se divide en cinco títulos y aborda en cada uno de ellos medidas de protección de los menores en diferentes contextos. La regulación prevista involucra a todos los grupos de interés afectados[85] y se enfoca de manera transversal a todos los ámbitos posibles con el objeto de conseguir una protección integral de los menores. Qué duda cabe que una correcta y completa protección de los menores en el universo digital solo puede conseguirse con el compromiso y la implicación de todas las partes interesadas. Es por ello por lo que, el Título I establece una serie de medidas dirigidas a los fabricantes. El Título II aborda medidas en el ámbito educativo. El Título III se dedica a fijar medidas en el ámbito de protección de las víctimas de violencia de género y sexuales. El Título IV prevé una serie de medidas en el ámbito sanitario. Y, finalmente, el Título V contempla una serie de medidas impuestas al sector público.

En relación con las medidas dirigidas a los fabricantes de dispositivos digitales y empresas tecnológicas el Proyecto de ley impone las siguientes obligaciones. En primer lugar, todos los dispositivos con acceso a Internet —*smartphones*, tabletas, televisores inteligentes, etc.— deberán incluir herramientas de control parental preinstaladas, activadas por defecto y gratuitas —art. 4.3 LOPMED—. Confiemos es que consigan instaurar medidas de control parental difíciles de sortear, ya que la mayoría de los adolescentes ya ha aprendido a esquivar estas restricciones. Esta circunstancia pone de manifiesto que la clave está en la educación digital y no solo en la regulación y en la restricción.

En España, la Ley Orgánica de Protección Jurídica del Menor y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales[86], reconocen el derecho de los menores al honor, a la intimidad personal y familiar, y a la propia imagen. Estos derechos incluyen la inviolabilidad de sus comunicaciones y datos personales. Sin embargo, los padres y tutores legales tienen la responsabilidad de proteger a sus hijos menores. Esta circunstancia justifica ciertas medidas de supervisión, siempre que se realicen de manera proporcional y con el objetivo de salvaguardar su bienestar. No obstante, debe encontrase un equilibrio, que no siempre es fácil, entre proteger debidamente al menor salvaguardando su derecho a la intimidad y su privacidad.

85. Participación de múltiples actores fabricantes, plataformas digitales, instituciones educativas y sanitarias en la protección de los menores.

86. La última modificación significativa de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales fue publicada el 9 de mayo de 2023 en el Boletín Oficial del Estado (BOE). Esta actualización ajustó la ley para alinearse con las correcciones del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En segundo lugar, queda absolutamente prohibida, la utilización de los datos personales de los menores por parte de los prestadores de servicios digitales para la elaboración de perfiles con fines comerciales, incluso cuando la persona usuaria adquiera la mayoría de edad —art. 4.3 *in fine* LOPMED—. En tercer lugar, los fabricantes deben incluir un etiquetado claro, al menos en el embalaje y en el libro de instrucciones, que advierta de los riesgos para la salud física y mental de los menores derivados del uso incorrecto de las nuevas tecnologías, por ejemplo, acceder a contenidos inapropiados para su edad[87].

En cuarto lugar, y con el objeto de prevenir conductas adictivas entre los menores, se prohíbe el acceso a mecanismos aleatorios de recompensa en videojuegos y otros juegos electrónicos, conocidos como "cajas botín" que permiten obtener premios virtuales —art. 5 LOPMED—.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales será el órgano encargado de velar por el cumplimiento de estas obligaciones por parte de los fabricantes. A tal efecto, realizará las labores de supervisión, control y realizará las oportunas inspecciones para garantizar el efectivo cumplimiento de estas obligaciones[88]. Se prevén sanciones por incumplimiento por importe de hasta dos millones de euros dependiendo de la gravedad y las consecuencias de la infracción. El ejercicio de la potestad sancionadora corresponde a la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales —art. 4.6 LOPMED—.

Por lo que se refiere a las medidas impuestas en el ámbito educativo —Título II—, se incorpora por primera vez la alfabetización digital en el currículo educativo desde educación primaria, abordando temas como privacidad, protección de datos y riesgos asociados al uso de redes sociales

87. El art. 4.2 del Proyecto de LOPMED establece: Obligaciones de los fabricantes de equipos terminales digitales con conexión a internet. "(…). 2. Los fabricantes de equipos terminales digitales referidos en el apartado anterior proporcionarán información en sus productos, al menos en el embalaje y en el libro de instrucciones, manual de usuario o guía de uso del equipo, en la que se advierta, en un lenguaje accesible, inclusivo y apropiado para todas las edades, de los riesgos derivados del acceso a contenidos perjudiciales para la salud y el desarrollo físico, mental y moral de las personas menores de edad. La obligación de información comprenderá, como mínimo, el siguiente contenido: a) Las medidas de protección de datos y los riesgos relacionados con la privacidad y la seguridad; b) el tiempo recomendado de uso de los productos y servicios, adecuado a la edad de la persona usuaria; c) los sistemas de control parental; d) los riesgos sobre el desarrollo cognitivo y emocional y la afección a la calidad del sueño de un uso prolongado de tales servicios".

88. Art. 4.5 del Proyecto de Ley Orgánica de Protección de menores en el entorno digital.

—art. 6 LOPMED—. Esta medida es clave ya que, si el objetivo es que los menores hagan un uso responsable de la tecnología, debemos enseñarles cómo utilizarla correctamente y no simplemente prohibirla. Esta alfabetización es una competencia clave para que los adolescentes tengan capacidad crítica y sean capaces de diferenciar y seleccionar fuentes fiables, ya que existe un exceso de información que lo hace cada vez más complicado[89]. Insistimos en la importancia de que los padres den un buen ejemplo a los menores en cuanto al uso de las nuevas tecnologías. Los centros educativos tendrán autonomía para regular el uso de dispositivos móviles en aulas y actividades extraescolares. —art. 7 LOPMED—. En la actualidad, ya se imparten en los centros educativos este tipo de cursos de formación en el ámbito digital, tanto para alumnos como para docentes. Sin embargo, el informe de la fiscalía General del Estado pone de manifiesto que no se está consiguiendo el objetivo perseguido. De ahí que resulte necesario incidir más e incorporarlo en el currículo educativo desde edades más tempranas[90].

En relación con el ámbito de la protección de las víctimas de violencia de género y violencia sexual en el entorno virtual adopta una serie de medidas en el Título III. En este sentido, la Ley establece que las personas menores de edad que sufran violencia de género o violencia sexual, a través de medios digitales, serán reconocidas como víctimas conforme a la Ley Orgánica 1/2004, de Medidas de Protección Integral contra la Violencia de Género, y la Ley Orgánica 10/2022, de garantía integral de la libertad sexual. Este reconocimiento asegura que las víctimas puedan acceder a los derechos y recursos previstos en estas normativas —arts. 8 y 9 RSD—.

Siguiendo con el carácter multidisciplinar de las medidas adoptadas por esta Ley, introduce reformas de gran calado en el Código Penal español para adaptarlo a las nuevas formas de criminalidad digital que afectan a menores. Estas modificaciones buscan fortalecer la protección de los menores frente a delitos cometidos en entornos digitales. A tal efecto, se implantan las órdenes de alejamiento digitales, que prohíbe la comunicación a través de plataformas digitales para condenados por delitos en línea. Esto es, impide a los agresores contactar con sus víctimas a través de medios digitales. Junto a ello, se tipifican como delitos el '*grooming*', esto es, la suplantación de identidad para fines sexuales. Y, finalmente, se penaliza la distribución de material pornográfico a menores.

89. FEIJOO, B., NÚÑEZ GÓMEZ, P., ÁLVAREZ FLORES, E.P. : "La alfabetización publicitaria…", cit. pp. 13-15.

90. *Vid.* el Capítulo V de la Memoria de la Fiscalía General del Estado 2024 está dedicado a "los menores y redes sociales", https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html.

Se incrementa de 14 a 16 años la edad mínima para que los menores puedan prestar consentimiento para el tratamiento de sus datos personales en redes sociales y otras plataformas digitales[91]. Esto es, se eleva la edad mínima para crearse una cuenta en redes sociales de 14 a 16 años. Esta modificación alinea a España con otros países de la Unión Europea que han establecido los 16 años como la edad mínima para el consentimiento en el tratamiento de datos personales[92]. Todavía no se sabe qué medidas se van a adoptar respecto de los menores que, a fecha de la entrada en vigor de la ley, ya dispongan de cuentas en las redes sociales. Entre otras cosas porque mientras no se disponga de mecanismos efectivos de verificación de la edad por parte de las plataformas, todas estas medidas resultan muy difíciles de implementar.

El Título IV aborda las medidas en el ámbito sanitario. Se establecen tanto medidas preventivas como medidas reactivas. En efecto, con el objeto de poder detectar de forma precoz cualquier problema derivado de un uso inapropiado de los dispositivos digitales incluirán revisiones pediátricas —art. 10 LOPMED—. Y, como medida reactiva se crearán centros especializados en salud mental para tratar adicciones tecnológicas —art. 11 LOPMED—.

El Título V se dedica a las medidas adoptadas en el sector público. Estas disposiciones reflejan el compromiso del sector público en la creación de un entorno digital seguro para los menores. Con el objeto de promover un uso seguro y responsable de las tecnologías digitales implementa una serie de políticas proactivas. A tal efecto, se desarrollarán campañas de información y sensibilización dirigidas a menores y sus familias, —art. 12 LOPMED—. Junto a ello, se prevé la colaboración con el sector privado para elaborar códigos de conducta que garanticen la protección de los menores en entornos digitales —art. 13 LOPMED—. Y, por supuesto, resulta absolutamente necesario un compromiso de formación continua de los profesionales que trabajan con menores —art. 14 LOPMED—.

Como conclusión, es de señalar que el Proyecto de Ley Orgánica de protección de los menores en los entornos digitales representa un avance significativo en la protección de los derechos de los menores. Al abordar el problema desde múltiples perspectivas y actualizar el marco legal, tiene el

91. La Disposición final VI de la LO Protección de menores en el entorno digital modifica el art. 7 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales que queda redactado como sigue: "1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años (…)".

92. Exposición de Motivos X de la LO Protección de menores en el entorno digital.

potencial de mejorar la seguridad y el bienestar de los menores en la red. Sin embargo, su éxito dependerá de la implementación efectiva de las medidas propuestas y de la colaboración entre el gobierno, las empresas tecnológicas, las instituciones educativas y las familias.

IV. NUEVOS MECANISMOS DE VERIFICACIÓN DE LA EDAD PARA EL ACCESO DE LOS MENORES A LOS SERVICIOS DIGITALES: EL REGLAMENTO (UE) 2024/1183, DE IDENTIDAD DIGITAL

A lo largo del trabajo ha quedado patente que resulta indispensable contar con mecanismos fiables de verificación de la edad con el objeto de poder proteger eficazmente a los menores en el mundo digital. La Unión Europea consciente de esta situación ha elaborado recientemente el Reglamento (UE) 2024/1183, de 11 de abril de 2024 sobre la identidad digital europea[93]. Este instrumento establece el marco europeo de identidad digital y es conocido por el acrónimo de sus siglas en inglés "eIDAS 2"[94] —*Electronic Identification, Authentication and Trust Services*—. *Este Reglamento* permite generar una cartera europea de identificación a través de un sistema fiable, universal y seguro de identidad digital.

La cartera digital será una aplicación móvil gratuita y voluntaria que permitirá a los usuarios almacenar y compartir credenciales de identidad —incluida la prueba de la mayoría de edad—. Asimismo, contendrá información identificativa como el DNI o el pasaporte y otros documentos relacionados con su identidad como permisos de conducción, credenciales educativas, permisos profesionales, cuentas bancarias o recetas médicas[95]. Esta nueva identidad digital permitirá a las personas acceder e identificarse en servicios en línea y fuera de línea, reduciendo trámites burocráticos con una tecnología de confianza[96]. Estas credenciales podrán utilizarse para

93. Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) núm. 910/2014, en lo que respecta al establecimiento del marco europeo de identidad digital, publicado en el DOUE el 30 de abril de 2024, conocido como "eIDAS2". Este Reglamento modifica el Reglamento (UE) 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, conocido como "eIDAS".

94. Las siglas "eIDAS" corresponden a *Electronic Identification, Authentication and Trust Services*, —Identificación Electrónica, Autenticación y Servicios de Confianza—.

95. https://ec.europa.eu/*EU Digital Identity Wallet Home — EU Digital Identity Wallet.*

96. TOMÁS MARTÍNEZ, G.: La discapacidad en la Cartera Europea de Identidad Digital (EUDI Wallet): Una oportunidad para mejorar la accesibilidad y contratos eficientes

validar la edad del usuario antes de registrarse en una red social de forma fiable y segura. De ahí que el sistema promete ser capaz de verificar la edad del usuario antes de acceder, ya sea de forma deliberada o accidental, a contenidos restringidos para menores. Además, el nuevo sistema no revelará la identidad, ni cualquier otra información personal adicional, a efectos de proteger la privacidad. El objetivo último es que el DNI digital sirva para funcionar con seguridad en el ámbito transfronterizo, ya sea para acceder a servicios públicos como privados[97]. Resulta del todo necesario conseguir su implementación lo antes posible teniendo en cuenta que algunas redes sociales con material pornográfico no impiden el acceso a menores o hay tutoriales para desbloquear el contenido para adultos[98].

El Reglamento establece que los usuarios tendrán control total sobre sus datos, decidiendo qué información comparten y con quién, sin seguimiento ni elaboración de perfiles en el diseño de las carteras. Sin embargo, aunque la cartera permite a los usuarios controlar la información que comparten, existe el riesgo de que algunos servicios o aplicaciones soliciten más datos de los necesarios.

Esta Cartera de Identidad Digital será expedida por cada uno de los Estados miembros de la Unión Europea. Para su elaboración cada Estado miembro deberá seguir las directrices y estándares comunes fijadas por la Unión Europea para garantizar la interoperabilidad y la confianza en el sistema[99]. El Reglamento eIDAS2 fija un plazo de 24 meses, desde su entrada en vigor para elaborar una cartera digital nacional que será reconocida en toda la UE y permitirá a los ciudadanos y empresas identificarse electrónicamente en toda la UE (EUDI *wallet*). El Reglamento entró en vigor el 20 de mayo de 2024[100] por lo que se espera que la implementación completa

(Disability in the European, Digital Identity Wallet (EUDI wallet): An opportunity to improve accessibility and efficient contracts) *Oñati Socio-Legal Series*, 2025. doi: 10.35295/osls.iisl.2217.

97. Algunos de los procesos que agilizará el uso de la Cartera de Identidad Digital serán la apertura de una cuenta bancaria, el pago de impuestos, la tramitación de cualquier solicitud administrativa o incluso almacenar una receta médica para poder utilizarla en cualquier lugar de Europa.

98. Informe del Consejo Audiovisual de Andalucía —CAA—: "La indefensión de los menores ante la pornografía en internet", *Cuadernos del Audiovisual*, 2024, p. 32.

99. https://digital-strategy.ec.europa.eu/es/policies/eudi-regulation?utm_source.

100. Tal y como dispone el art. 2 del Reglamento Reglamento (UE) 2024/1183 (eIDAS 2): "El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". El Reglamento fue publicado en el DOUE el 30 de abril de 2024.

de esta tecnología esté lista antes de finales de 2026 en todos los Estados miembros. Este plazo de 24 meses pretende dar un margen suficiente a los Estados y a los prestadores de servicios digitales[101] preparar y adaptar sus sistemas para aceptar este tipo de certificados de edad. En definitiva, el objetivo que persigue es, por un lado, que el acceso de los menores a contenido inapropiado quede automáticamente bloqueado. Y, por otro lado, que les impida registrarse en redes sociales para las que no tienen la edad mínima requerida.

Es evidente que el Reglamento de identidad digital presenta numerosas ventajas, como hemos visto, al tener como objetivo mejorar la seguridad, privacidad e intimidad de los usuarios, así como agilizar todos sus trámites. Sin embargo, la cartera digital europea, al igual que cualquier avance tecnológico, conlleva ciertos riesgos. A saber, por un lado, el hecho de centralizar todos los datos personales en una sola cartera digital puede convertirla en un objetivo atractivo para los *ciber* delincuentes convirtiendo los datos personales en altamente vulnerables. Por otro lado, la adopción generalizada de la cartera digital implicaría una dependencia tecnológica absoluta de los ciudadanos para realizar cualquier trámite. De ahí que, si surge cualquier problema técnico que impide el acceso a la misma, podría tener graves consecuencias para los usuarios. Junto a ello, resulta absolutamente necesario implementar medidas de protección adecuadas, para evitar que los gobiernos utilicen estas carteras para rastrear y monitorear las actividades de los ciudadanos en línea.

Teniendo en cuenta que ya ha transcurrido justo un año desde la entrada en vigor del Reglamento 2024/1183 eIDAS2, vamos a ver qué iniciativas se están llevando a cabo en España para cumplir con las disposiciones del mismo. En primer lugar, el Ministerio para la Transformación Digital y de la Función Pública está desarrollando una Cartera Digital nacional Beta, en línea con la medida 4 del Eje 1 del Plan de Digitalización 2021-2025[102].

Esta iniciativa busca proporcionar a los ciudadanos un medio seguro y sencillo para identificarse electrónicamente, facilitando la interoperabilidad con otros sistemas europeos y adaptándose al nuevo marco establecido por el Reglamento eIDAS 2.

---

101. REIG FABADO, I.: "La adaptación del derecho de la competencia europeo a la 'era digital': algunos aspectos de la propuesta legislativa para las grandes plataformas digitales", en CASTELLÓ PASTOR, J.J. (Dir.): *Desafíos jurídicos ante la integración digital: Aspectos europeos e internacionales,* Aranzadi (Thomson Reuters), 2021, p. 238.
102. Para más información al respecto vid: 210127_plan_digitalizacion_administraciones_publicas.pdf y https://carteradigital.gob.es/

En segundo lugar, el Consejo de Ministros aprobaba el 1 de abril de 2025 un Real Decreto que regula el proceso de expedición, gestión y desarrollo del documento nacional de identidad digital (DNI). A tal efecto, el Gobierno ha lanzado recientemente la aplicación oficial 'miDNI'[103] que ofrece a la ciudadanía la posibilidad de disponer del documento de identidad en formato digital en sus dispositivos móviles[104]. De este modo, adapta el uso del DNI a los nuevos retos digitales. Si bien, en una primera fase, el DNI digital no servirá para acreditar la identidad, ni la edad de los usuarios en la red quedando limitado a la identificación presencial dentro del país. Será en una segunda fase, prevista para mediados de 2026 —fecha en la que el Reglamento (UE) 2024/1183 (eIDAS 2) debe ser plenamente aplicable— cuando la aplicación MiDNI permitirá la acreditación de la identidad y de la edad para hacer todo tipo gestiones telemáticas. Será a partir de ese momento cuando los menores podrán acreditar su edad de forma efectiva y fiable para poder acceder, en su caso, a los servicios digitales aptos para su edad quedando correctamente protegidos en el entorno digital.

En tercer lugar, es de señalar que España participa activamente en proyectos europeos como *Digital Credentials For Europe* (DC4EU)[105] y EBSI *Nodes Expansion* (EBSI-NE)[106], que buscan establecer un marco común para la emisión y verificación de credenciales digitales utilizando una tecnología común en el ámbito de la UE. La participación de España en estos proyectos se estima fundamental para la implementación de la Cartera Digital Europea y garantizar su interoperabilidad entre los Estados miembros. demuestran un firme compromiso con la implementación del Reglamento eIDAS 2.

Finalmente, el Ministerio para la Transformación Digital y de la Función Pública está trabajando activamente en la implementación de los mecanismos de verificación de la edad para dar cumplimiento a las normas europeas. A tal efecto, ha desarrollado una serie de documentos técnicos[107] que establecen el marco para la verificación de edad en entornos digitales. El primer documento, denominado "Presentación del Ecosistema de Verificación de Edad" desarrolla un sistema que permite verificar la mayoría de edad de los usuarios en línea, protegiendo en todo momento los derechos fundamentales de los menores con el interés superior del menor como prioridad. El segundo de ellos denominado "Protocolo de Verificación de Edad para

103. Para más información al respecto vid: Portal MiDNI.
104. Para más información visitar: Ministerio del Interior | El Gobierno aprueba la expedición del DNI digital.
105. Para más información al respecto vid: https://www.dc4eu.eu/
106. Para más información al respecto vid: https://www.ebsi-ne.com/
107. https://digital.gob.es/especificaciones_tecnicas

las Plataformas que se Integran con el Sistema" prevé las especificaciones técnicas que deberán cumplir las plataformas para permitir la verificación de la mayoría de edad de los usuarios mediante la presentación de credenciales emitidas por la Cartera Digital. Y el tercero: "Especificación de Uso de la Credencial de mayoría de Edad en Cartera Digital BETA" La Cartera Digital BETA emite credenciales seguras de verificación de la edad. Para dotar de mayor seguridad al sistema, establece mecanismos de doble autenticación preservando en todo momento la identidad de los usuarios.

V. CONCLUSIONES

En un mundo donde la digitalización avanza a pasos agigantados se abren oportunidades sin precedentes para el desarrollo educativo, social y cultural de todos los usuarios, en especial para los menores. No obstante, como contrapartida los menores están cada vez más expuestos a toda una serie de riesgos que comprometen no solo su intimidad, sino también su integridad física, emocional y moral, por no hablar del enorme poder de manipulación que ejerce la publicidad digital sobre los menores. La especial vulnerabilidad de los menores exige un marco normativo reforzado que garantice una protección integral de sus derechos fundamentales en el entorno digital al igual que ocurre en el entorno físico. En este contexto es donde la Unión Europea y los Estados juegan un papel determinante, no solo elaborando normativa, sino estableciendo mecanismos eficaces que aseguren el cumplimiento de la misma y previendo la imposición de sanciones para el caso de incumplimiento.

El análisis del marco jurídico europeo y estatal revela avances significativos y reflejan el compromiso del sector público en la creación de un entorno digital seguro para los menores, mediante la implementación de políticas proactivas, la colaboración con el sector privado y la formación continua de los profesionales involucrados. En efecto, es imprescindible destacar que la protección jurídica de los menores en el entorno digital no puede depender exclusivamente del legislador o de las plataformas tecnológicas. La corresponsabilidad de los progenitores, tutores legales, educadores y de la sociedad en su conjunto es fundamental para fomentar una ciudadanía digital crítica, segura y responsable. Junto a ello, la alfabetización digital, la educación afectivo-sexual, la formación sobre privacidad y el uso ético de la tecnología deben integrarse en el currículo educativo de forma transversal para lograr el desarrollo integral del menor.

A lo largo del trabajo se ha puesto de manifiesto como el elemento clave para una protección efectiva de los menores radica en implementar mecanis-

mos fiables de verificación de la edad de los menores en el entorno digital. Afortunadamente, después de mucho esfuerzo todo apunta a que en breve dispondremos de un sistema fiable en la Unión Europea. En efecto, el Reglamento sobre la identidad digital europea (EUDI) revolucionará la identidad digital en la Unión Europea al permitir la creación de una cartera europea de identidad digital universal, fiable y segura. Este mecanismo promete verificar la edad de forma efectiva y, a su vez, preservando la identidad y privacidad de los menores. De este modo, plantea nuevas vías para salvaguardar el interés superior del menor, permitiendo limitar el acceso a contenidos inapropiados y garantizando entornos digitales acordes con su etapa de desarrollo. Esperemos que haya una amplia aceptación y uso generalizado de estas nuevas herramientas digitales. No obstante, ello dependerá de realizar campañas de sensibilización y formación adecuadas para la ciudadanía.

Finalmente, el Proyecto de Ley Orgánica de Protección de los Menores en los Entornos Digitales, cuya entrada en vigor se prevé en breve, en España supone un avance significativo en la protección de los derechos de los menores. Ello es así por cuanto que el nuevo texto legislativo aborda el problema desde múltiples perspectivas con el objeto de conseguir una protección integral de los menores en el entorno digital. Sin embargo, su verdadero éxito dependerá de la implementación efectiva de las medidas propuestas y de la colaboración entre el gobierno, las empresas tecnológicas, las instituciones educativas y las familias.

BIBLIOGRAFÍA

ANDRADE, B., GUADIX, I., RIAL, A. Y SUÁREZ, F.: "Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades", Informe de UNICEF, Madrid, 2021, pp. 1-106.

CASTELLÓ PASTOR, J.J. "Interrelación del Reglamento de servicios digitales con el Reglamento Platform to Business (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, en CASTELLÓ PASTOR, J.J. (Dir.), Aranzadi (Thomson Reuters), 2024, pp. 361 y ss.

CASTELLÓ PASTOR, J.J., Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea, *Cuadernos de derecho transnacional*, Vol. 17, N.º 1, 2025, págs. 308-328.

CATALINA GARCÍA, B., LÓPEZ DE AYALA, M.C., GARCÍA JIMÉNEZ, A.: "Los riesgos de los adolescentes en internet: los menores como actores y víctimas de los peligros de Internet", *Revista Latina de Comunicación Social*, 2014, pp. 462-485.

DE MIGUEL ASENSIO, P. : *"Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales", La ley Unión Europea*, núm. 109, dic. 2022, pp. 1-47.

DE MIGUEL ASENSIO, P. : "Protección de menores en línea (I): Directrices relativas al artículo 28(4) del Reglamento de Servicios Digitales", publicado el 31 de mayo de 2025 en: https://pedrodemiguelasensio.blogspot.com/2025/05/proteccion-de-menores-en-linea-i.html

FEIJOO, B., SÁDABA, C.: When Ads Become Invisible: Minors' Advertising Literacy While Using Mobile Phones, *Media and Communication*, 2022, Vol. 10, Issue 1, https://doi.org/10.17645/mac.v10i1.4720.

FEIJOO, B., NÚÑEZ GÓMEZ, P., ÁLVAREZ FLORES, E.P. : "La alfabetización publicitaria de niños y adolescentes ante los nuevos formatos digitales", Revista Científica de Comunicación Aplicada, núm. 15(1), 2025, pp. 13-29.

FERRER-LÓPEZ, M.: "Neuromarketing y la medición del efecto de la publicidad de influencers en adolescentes", *Revista Mediterránea de la Comunicación/Mediterranean Journal of Communication*, 11(2), pp. 241-259. https://www.doi.org/10.14198/MEDCOM2020.11.2.11

GARCÍA GARNICA, M.: "Datos personales y menores de edad", en *Protección de datos personales, Asociación de Profesores de Derecho civil,* Tirant Lo Blanch, 2020.

HERRERA DE LAS ERAS, R., PAÑOS PÉREZ, A.: *La privacidad de los menores en las redes sociales. Especial consideración al fenómeno influencer*, Atelier, 2022.

MARTÍNEZ, G., GARMENDIA, M., GARITAONANDIA, C.: "La infancia y la adolescencia ante las tecnologías de la información y la comunicación (TIC): oportunidades, riesgos y daño", *Zer*, 2020, 25 (48), pp. 349-362.

MÉNDEZ SUÁREZ, M., SIMÓN MOYA, V. Y MUÑOZ DE PRAT, J.M.: "Do current regulations prevent unethical AI practices?", *Journal of Competitiveness*, 15(3), 2023, pp. 207-222, https://doi.org/10.7441/JOC.2023.03.11

MORALEJO IMBERNON, N.: *Los derechos de los menores y las redes sociales*, Valencia, Tirant lo Blanch, 2023.

MORENO PIZARRO, E., RIVERO HERNÁNDEZ, F.: *El interés superior del menor: Claves jurisprudenciales,* Ed. Reus, 2020.

MORILLAS FERNÁNDEZ, M.: "Menores vulnerables y redes sociales: nuevos retos jurídicos en la protección ante el uso inadecuado: edad, educación y controles por defecto", *Revista Internacional de Doctrina y Jurisprudencia*, vol. 32, dic. 2024, pp. 47-70.

NÚÑEZ GÓMEZ, P., ORTEGA MOHEDANO, F., LARRAÑAGA MARTINEZ, K.: "Hábitos de uso y consumo de pantallas inteligentes entre niños/as de 7 a 9 años en España", *Revista Mediterránea de Comunicación,* 12 (1), 2021, pp. 191-204.

PALFREY, J., & GASSER, U.: *Born digital: Understanding the first generation of digital natives,* 2008, Basic Books/Hachette Book Group.

REIG FABADO, I.: "La adaptación del derecho de la competencia europeo a la 'era digital': algunos aspectos de la propuesta legislativa para las grandes plataformas digitales", en CASTELLÓ PASTOR, J.J. (Dir.): *Desafíos jurídicos ante la integración digital: Aspectos europeos e internacionales,* Aranzadi (Thomson Reuters), 2021, pp. 227-260.

REIG FABADO, I.: "Las VLOPs y los riesgos sistémicos en la DSA: algunos aspectos problemáticos", en *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, en CASTELLÓ PASTOR, J.J. (Dir.), Aranzadi, 2024, pp. 283-324.

RODRIGO MARTÍN, L., RODRIGO MARTÍN, I., MUÑOZ SASTRE, D.: "Los influencers virtuales como herramienta publicitaria en la promoción de marcas y productos. Estudio de la actividad comercial de Lil Miquela", *Revista Latina de Comunicación Social,* núm. 79, 2021, pp. 60-90.

SERRANO-MAÍLLO, I.: "Menores y contenidos digitales. Derechos y obligaciones", *Revista Mediterránea de Comunicación,* vol. 13 (1), pp. 107-122.

TOMÁS MARTÍNEZ, G.: La discapacidad en la Cartera Europea de Identidad Digital (EUDI Wallet): Una oportunidad para mejorar la accesibilidad y contratos eficientes (Disability in the European, Digital Identity Wallet (EUDI wallet): An opportunity to improve accessibility and efficient contracts) *Oñati Socio-Legal Series*, 2025.

Capítulo 3

Evolución de la regulación de los "Dark Patterns" en la Unión Europea*

José Corberá Martínez
Prof. Contratado Dr. de Derecho Mercantil (acr. a Titular)
Departamento de Economía y Ciencias Sociales, DECS.
Universitat Politècnica de València (UPV)
Miembro del CEGEA

SUMARIO: I. INTRODUCCIÓN. 1. *Impacto socioeconómico de las nuevas tecnologías*. 2. *Importancia de los interfaces de usuario en línea como* "front office" *del comercio digital*. 3. *Objeto: aproximación al concepto y a la regulación europea sobre interfaces engañosas*. II. CONCEPTO Y TIPOS DE INTERFACES ENGAÑOSOS. 1. *Precisiones terminológicas*. 2. *Concepto de* "Dark Patterns". 3. *Breve referencia a los tipos de interfaces engañosas y patrones oscuros*. III. REGULACIÓN VIGENTE. 1. *Reconocimiento de los "patrones oscuros" en interfaces de usuarios en la Comunicación sobre la Nueva Agenda del Consumidor de 2020*. 2. *Reglamento de Servicios Digitales de 2022 como primera regulación expresa de las interfaces engañosas en la Unión Europea*. 2.1. Ámbito de aplicación. 2.2. Articulación con la Directiva de Prácticas Coe merciales Desleales con Consumidores y del Reglamento General de Protección de Datos. 3. *Directiva sobre las Prácticas Comerciales Desleales de 2005*. 4. *Reglamento General de Protección de Datos de 2016*. 5. *Reglamento de Mercados Digitales de 2022*. 6. *Reglamento de Datos de 2023*. 7. *Directiva de Servicios Financieros a Distancia de 2023*. 8. *Reglamento de Inteligencia Artificial de 2024*. 9. *Necesidad de mayor*

* Esta publicación es parte del Proyecto "Hacia una transición digital centrada en la persona en la Unión Europea" TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro el autor.

cohesión de la normativa reguladora de las "Dark Patterns". IV. REGULACIÓN FUTURA SOBRE "EQUIDAD DIGITAL". V. A MODO DE CONCLUSIÓN. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

1. IMPACTO SOCIOECONÓMICO DE LAS NUEVAS TECNOLOGÍAS

En otro momento y lugar, se ha expresado que, entre las diversas aproximaciones que intentan caracterizar la sociedad actual destacan las que la califican en atención a la importancia socioeconómica de la información[1] y del conocimiento[2] hilvanado con el empleo intensivo de las nuevas tecnologías que, además, aumentó con la crisis sanitaria mundial ocasionada por la irrupción de la pandemia iniciada en 2020, que aceleró la transformación digital. A la fecha, el panorama socioeconómico se caracteriza también, entre otros aspectos, por la creciente digitalización de múltiples facetas de la vida humana entre las que se encuentran aquellas que, con relieve jurídico, inciden en el ámbito del empresario, de la empresa y del mercado, pilares sustantivos fundamentales del Derecho mercantil. Fenómenos como la digitalización del curso empresarial, el notable posicionamiento del comercio digital y de las plataformas de contenidos digitales, así como el auge de los criptoactivos dan cuenta de esta realidad que, tal vez, se aprecia de forma paradigmática en el incesante aumento del empleo de aplicaciones basadas en la inteligencia artificial, lo que ha propiciado que voces de ámbitos metajurídicos caractericen a la sociedad actual a través de las incidencias de la tecnología en el poder de decisión y la denominada "mercantilización integral de la vida"[3].

---

1. Entre otros *vid.* MACHLUP, F., *The production and distribution of knowledge in the United States*, Princeton University Press, Princeton, NY, 1962, pp. 1-416; BELL, D., *The Coming of Post-Industrial Society. A Venture in Social Forecasting*, Basic Books, New York, 1973, pp. 1-507; y MASUDA, Y., *The Information Society as Post Industrial Society*, Institute for the Information Society, Tokyo, Japan, 1980, pp. 1-158, y World Future Society, Washington, D.C., 1981, pp. 1-178.
2. Para una aproximación a la configuración del concepto "sociedad del conocimiento", *vid.* DRUCKER, P. F., *The age of discontinuity. Guidelines to Our Changing Society*, William Heinemann, London, 1969, pp. 152-154, y HAYEK, F. A., *The Use of Knowledge in* Society, *American Economic Review,* XXXV, N.º 4, 1945, pp. 519-530.
3. *Vid.* SADIN, E., *La humanidad aumentada*, Caja Negra, Ciudad Autónoma de Buenos Aires (Argentina), 2017, pp. 1-160.

2. IMPORTANCIA DE LOS INTERFACES DE USUARIO EN LÍNEA COMO "*FRONT OFFICE*" DEL COMERCIO DIGITAL

En este contexto cobran especial importancia las nuevas formas de interacción entre algoritmos o aplicaciones y personas a través de las denominadas interfaces de usuario y de experiencia que ofrecen diferentes terminales que actúan como soporte, toda vez que van a encarnar la faceta perceptible (por visible a las personas) que articulará cada interacción. Dicho de otra forma, las interfaces de usuario permiten a las personas la toma de decisiones. En este sentido, actuarán con el *front office* de prestaciones *on line*, de ahí la importancia de las mismas y, en lo que ahora interesa, de su diseño.

La importancia, tanto de las interfaces en línea como de su diseño se ha evidenciado de manera clara e inequívoca en la regulación que, sobre estos aspectos, contempló el legislador europeo por primera vez de manera expresa en el art. 25 del Reglamento de Servicios Digitales de 2022[4], sobre el diseño y organización de los interfaces en línea[5]. Es oportuno recordar también que el citado Reglamento ofreció en su art. 3 la definición de "interfaz en línea" entendida como "todo programa informático, incluidos los sitios web o partes de sitios web, y las aplicaciones, incluidas las aplicaciones móviles". Sin embargo, es el art. 25 del Reglamento de Servicios Digitales la norma llamada a regular de manera expresa por primera vez, las denominadas interfaces engañosas, también conocidos como patrones oscuros o en su traducción al inglés: *"Dark Patterns"*.

Ahora bien, el artículo 25 del Reglamento de Servicios Digitales no agota la regulación de los patrones oscuros, sino que está llamado a cohesionarse con otros instrumentos normativos europeos pensados para un mundo analógico, pero con fácil encaje en el ámbito *on line*. Todo ello sin perjuicio de la posible aplicabilidad de otras ramas del Derecho como puede suceder con respecto a la afectación del Derecho de la competencia de la Unión Europea que puede ocasionar aquellos *"Dark Patterns"* que constituyan un abuso de posición dominante en los términos del artículo 102 del Tratado de Funcionamiento de la Unión Europea[6]. Se trata ahora

4. Reglamento (UE) 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 (DOUE L 277/1, de 27.10.2022) (en adelante "Reglamento de Servicios Digitales" o "RSD").

5. *Vid*. además del art. 25 RSD sobre "Diseño y organización de interfaces en línea", el art. 26 sobre "Publicidad en las plataformas en línea", y el art. 31 que regula el "Cumplimiento desde el diseño".

6. Tratado de Funcionamiento de la Unión Europa (2016/C 202/01) (DOUE C 202/1, de 7.6.20216) (en adelante "TFUE"). Sobre la cuestión en la doctrina internacional, entre

de otras normativas como la que tutela la protección de los consumidores frente a prácticas comerciales desleales[7], la correspondiente a la protección de datos[8], así como a su acceso justo y utilización[9], la propia de los mercados digitales[10] u otras más dispares como la que ordena los contratos de servicios financieros a distancia[11], y —más recientemente—, la relativa a la inteligencia artificial[12], pero que también prestan atención de forma expresa o implícita a los patrones oscuros en los interfaces en línea por sí mismo, pero sobre todo por los intereses que pueden afectar, que bien pueden sintetizarse en esta introducción en la relevancia de preservar la toma de decisiones libre.

---

otros *vid*., DAY, G., and STEMLER, S., "Are dark patterns anticompetitive", *Alabama Law Review*, Vol. 72:1:1, 2020, pp. 1-45, y CAUFFMAN, C., KAMPERMAN SANDERS, A., and TYAGI, K. (eds.), Digital Platforms, Competition Law, and Regulation: Comparative Perspectives, Hart Publishing, London, 2024, pp. 1-246.

7. En particular, se trata de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo (DOUE L 149/22, de 11.6.2005) (en adelante "Directiva sobre las prácticas comerciales desleales" o "DPCD").
8. En concreto, a través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE L 119/1, de 4.5.2016) (en adelante "Reglamento General de Protección de Datos" o "RGPD").
9. Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (DOUE L, de 22.12.2023 (en adelante "Reglamento de Datos" o "RD").
10. Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (DOUE L 265/1, de 12.10.2022) (en adelante "Reglamento de Mercados Digitales" o "RMD").
11. Se trata de la Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023, por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia y se deroga la Directiva 2002/65/CE (DOUE L, de 28.11.2023) (en adelante "Directiva de Servicios Financieros a Distancia" o "DSFD").
12. En concreto, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (DOUE L, de 12.7.2024) (en adelante "Reglamento de Inteligencia Artificial" o "RIA").

No ha de extrañar que, recientemente, algunas voces en la doctrina internacional[13] hayan puesto de manifiesto que regulación de los patrones oscuros se haya convertido en un tema de creciente importancia, por tratarse de prácticas engañosas en línea por las que se manipula a los usuarios para que realicen acciones que no redundan en su beneficio, mediante innumerables tácticas avanzadas por las que, en definitiva, ocultar la transparencia. Como se dijo, la importancia del tratamiento legal de las interfaces engañosas encuentra reflejo en el incremento de instrumentos legales que en el ámbito de la Unión Europea ofrecen regulación aplicable, a la que, previsiblemente, se tiene que añadir, en su caso, una futura *Digital Fairness Act*[14], lo que sin lugar a duda también plantea diversas dudas jurídicas a la luz de los posibles solapes y vacíos que puede ocasionar[15].

3. OBJETO: APROXIMACIÓN AL CONCEPTO Y A LA REGULACIÓN EUROPEA SOBRE INTERFACES ENGAÑOSAS

Con carácter general, el objeto del presente trabajo se centra en desarrollar de forma sintética la evolución de la legislación europea en materia de interfaces engañosas conocidas como *"Dark Pattens"* o "patrones oscuros", para identificar ventajas y desventajas de la regulación vigente que resulta de aplicación y con miras a la futura legislación contenida en la Directiva de Equidad Digital o *Digital Fairness Act*, por las que ofrecer diversas conclusiones a modo de aspectos a considerar en a la hora de acometer la ordenación jurídica del fenómeno de las interfaces engañosas en el contexto de la Unión Europea y de nuestro ordenamiento jurídico. Para alcanzar tal propósito se desarrolla en los siguientes apartados la evolución las normas que regulan los interfaces engañosos de manera cohesionada con objetivos de política jurídica de cada normativa específica. Asimismo, se describen propuestas doctrinales de perfeccionamiento en la articulación de las en el Derecho de la Unión Europea para intentar mejorar la eficacia de las normas jurídicas y a la consecución de sus objetivos, entre los que destaca la protección de los Derechos del consumidor en el contexto digital. En consecuencia, el objeto de este trabajo se puede sintetizar en aproximar la noción de *"Dark Patterns"*

13. *Vid.* HERMAN J., Dark patterns: EU's regulatory efforts. *Security and Privacy*. 2024; 7(6): 441, pp. 1-14.
14. *Vid.* portal web de la Comisión Europea dedicado a esta iniciativa, EUROPEAN COMMISSION, Digital fairness — fitness check on EU consumer law (disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en) (último acceso: 3.7.2025).
15. *Vid.* HERMAN J., Dark patterns: EU's regulatory efforts. Security and Privacy, ob. cit., pp. 1-14.

como interfaces engañosas y la evolución de la regulación de las mismas en la legislación europea, con el fin de contrastar la idoneidad de la normativa europea vigente en relación con la tutela del consumidor, a la que se añadirá la futura normativa de aplicación en materia de equidad digital.

II. CONCEPTO Y TIPOS DE INTERFACES ENGAÑOSOS

1. PRECISIONES TERMINOLÓGICAS

Es fácil advertir la existencia de diversos términos empleados para designar los interfaces de usuario diseñados con la finalidad de manipular a los consumidores. En particular, mientras la doctrina en un origen acuñó la expresión *"Dark Patterns"*, en los textos legales coexistirá con la referente a los *"Deceiptive Patterns"*. Lo mismo es de ver en las traducciones al español en las que se hace referencia a los "patrones oscuros" o a los "patrones engañosos", por lo que se estima oportuno precisar en este momento que se utilizarán indistintamente los anteriores términos por remitir al mismo fenómeno, que bien se puede resumir en la existencia de patrones oscuros en las interfaces, en alusión a la finalidad engañosa orientada a manipular con la fueron diseñadas.

2. CONCEPTO DE "*DARK PATTERNS*"

El concepto de *"Dark Patterns"* entendido como "patrones oscuros" cuenta con antecedentes ajenos al ámbito de las interfaces de usuario, toda vez que se trata de la expresión con la que se han identificado algunas conductas desarrolladas en varios ámbitos comerciales como el correspondiente al posicionamiento producto en los supermercados con el fin de llamar la atención y ganarse el favor de la clientela. Semejante finalidad se observará en el contexto de las nuevas tecnologías e internet, ya no solo para decantar una decisión económica consistente, por ejemplo, en la contratación de prestaciones, sino también en relación con la gestión y la protección de datos[16].

16. En este sentido, la Agencia Española de Protección de Datos (AEPD), explica que las "Dark Patterns" son "interfaces e implementaciones de experiencia de usuario destinadas a influenciar en el comportamiento y las decisiones de las personas en su interacción con webs, apps y redes sociales, de forma que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales". *Vid.* portal web de la Agencia Española de Protección de Datos (AEPD), Entrada "*Dark patterns*: Manipulación en los servicios de Internet", de 19.5.2022 (disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet) (última consulta: 2.7.2025).

En el ámbito de la Unión Europea, a la fecha, es el propio Reglamento de Servicios Digitales el que en su Cdo. 67 ofrece una definición de *"Dark Patterns"* al explicar que "(l)os patrones oscuros en las interfaces en línea de las plataformas en línea son prácticas que distorsionan o perjudican materialmente, ya sea de propósito o de hecho, la capacidad de los destinatarios del servicio para tomar decisiones o elecciones autónomas e informadas (…)". Esta orientación sigue la que formuló la Comunicación de la Comisión Europea, "Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible"[17], de forma sintética, en el año 2020, por la que se hace referencia a "(d)iseños de interfaces de usuario que tienen la finalidad de manipular a los consumidores".

Sin embargo, parece oportuno recordar que para encontrar el origen comúnmente aceptado de "Dark Patterns", en relación con las interfaces[18] hay que remontarse al empleo del mismo en el año 2010 por Harry BRINGNULL, en el espacio web titulado "Dark Patterns: User Interfaces Designed to Trick People"[19], en el que se describe como "(n)ormalmente cuando se piensa en 'mal diseño', se piensa en pereza o errores. Estos se conocen como anti-patrones de diseño. Los patrones oscuros son diferentes: no son errores, están cuidadosamente elaborados con una sólida comprensión de la psicología humana y no tienen en mente los intereses del usuario"[20]. No obstante, el concepto de *"Dark Pattern"*, como patrón oscuro, ha virado hacía la noción de *"Deceiptive Pattern"* entendida como

17. Comunicación de la Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Nueva Agenda del Consumidor Reforzar la resiliencia del consumidor para una recuperación sostenible, Bruselas, 13.11.2020 COM (2020) 696 final (en adelante "Comunicación de 2020").

18. *Vid*. OECD, "Dark commercial pattern", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, 2022, pp. 7 y ss., así en la reciente doctrina en nuestro ordenamiento jurídico, *vid*., y, asimismo, MATO PACÍN, M.ª, N., *Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros*, Agencia Estatal Boletín Oficial del Estado, Colección Derecho Privado 29, Madrid, 2024, pp. 51 y 52.

19. *Vid*. web "Dark Patterns" de 2010, disponible en: https://old.deceptive.design/main_page/index.html (fecha de consulta: 10.12.2023). En la actualidad, *vid.* BRIGNULL, H., LEISER, M., SANTOS, C., & DOSHI, K. (2023, April 25). *Deceptive patterns — user interfaces designed to trick you*. deceptive.design. Retrieved April 25, 2023, from https://www.deceptive.design/ (última consulta: 3.7.2025).

20. *Vid*. BRINGNULL, H., web "Dark Patterns" de 2010, antes disponible en: https://old.deceptive.design/main_page/index.html (última consulta: 3.7.2025). Traducción libre: "Normally when you think of 'bad design', you think of laziness or mistakes. These are known as design anti-patterns. Dark Patterns are different — they are not mistakes, they are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind".

patrón engañoso[21]. Es por ello por lo que, en la actualidad, se afirma que los patrones engañosos son equivalentes a los "patrones oscuros" por consistir, en suma, en "trucos utilizados en sitios web y aplicaciones que te hacen hacer cosas que no era tu intención, como comprar o registrarte en algo"[22]. Por otra parte, la doctrina internacional especialista en la materia ha formulado la siguiente definición de patrones oscuros *"Dark Patterns"* o diseños engañosos *"Deceiptive Designs"* entendidos como "prácticas que manipulan o explotan a los usuarios para llegar a resultados específicos, a menudo a expensas de su autonomía, juicios, tomas de decisiones o elecciones"[23]. Finalmente, algunas voces en la doctrina han advertido que "(n)o hay una única definición aceptada de patrones oscuros, pues se trata de un concepto amplio que engloba muchas prácticas diferentes"[24]. Con todo, bien puede acogerse la definición formulada en la Comunicación de 2020 sobre la Nueva Agenda del Consumidor que define los patrones oscuros como los "(d)iseños de interfaces de usuario que tienen la finalidad de manipular a los consumidores", para lleven a cabo una determinada conducta económica o relativa al tratamiento de sus datos.

3. BREVE REFERENCIA A LOS TIPOS DE INTERFACES ENGAÑOSAS Y PATRONES OSCUROS

En la actualidad existen multitud de ejemplos constitutivos de interfaces engañosas o *"Dark Patterns"*. A la fecha, se afirma que no existe una clasificación oficial o que sea fruto del consenso, sino un conjunto de listados de prácticas catalogadas como patrón oscuro elaborados por sectores de la doctrina sobre diversos criterios[25]. No obstante, a efectos de aproximar la tipología de patrones oscuros[26] es oportuno recordar la tipología ha evolu-

21. *Vid.* LEISER, M. and SANTOS, C., *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface* (April 27, 2023), p. 2, al incidir en el carácter intercambiable de los términos.
22. *Vid.* BRIGNULL, H., LEISER, M., SANTOS, C., & DOSHI, K., ob. cit. (traducción libre).
23. *Vid.* LEISER, M. and SANTOS, C., *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface*, ob. cit., p. 2 al explicar del concepto: "These patterns may range from subtle nudges to overtly coercive tactics that deceive or trick users into taking specific actions that benefit the platform or service provider. The use of dark patterns has become a growing concern".
24. *Vid.* MATO PACÍN, M.ª, N., *Aspectos jurídicos del diseño de las interfaces digitales*, ob. cit., p 52., apud. KAPROU, E., "Aggressive commercial practices 2.0: Is the UCPD fit for the digital age?", *Journal of European Consumer and Market Law*, no. 2, 2023, p. 80.
25. *Ibid.*, p. 53.
26. No obstante, existen recientes y acertadas aproximaciones en la doctrina nacional, como es de ver en CASADO, A., *Prácticas desleales en entornos digitales*, Tirant Lo Blanch, Valencia, 2025, pp. 97 y ss., en relación con el concepto y taxonomía.

cionado, en atención al crecimiento de prácticas calificadas como patrones oscuros. En su origen, entre las primeras conductas identificadas por Harry BRINGNULL se encuentran las identificadas con las siguientes denominaciones[27]: *Bait and Switch*[28], *Disguised Ads*, *Faraway Bill*, *Forced Continuity*[29], *Forced Disclosure*, *Friend Spam*[30], *Hidden Costs*[31], *Misdirection*[32], *Price Comparison Prevention*, *Privacy Zuckering*, *Roach Motel*, *Road Block*, *Sneak into Basket*, y *Trick Question*. Posteriormente, en recientes revisiones de las clases de conductas[33] se identificaron más patrones que pasaron a engrosar el catálogo de las *"Dark Patterns"*[34].

III. REGULACIÓN VIGENTE

La regulación vigente de los interfaces engañosos, en la actualidad, encuentra un hito relevante en la regulación contenida en la Reglamento

27. *Vid.* BRINGNULL, H., web "Dark Patterns" de 2010, ob. cit., seguida en este punto.
28. *Vid. ult. loc.*, al remitir a los supuestos de "venta con señuelo", en los que el usuario pretende realizar un acto, pero sucede algo diferente y no deseado, es una práctica que admite muchas variantes en la práctica.
29. Realizadas por BRIGNULL, LEISER, SANTOS, y DOSHI, *Vid.* BRINGNULL, H., web "Dark Patterns" de 2010, ob. cit., se trata del supuesto de continuidad forzosa que se da en los supuestos de registro o suscripción en los que se solicitan los datos de tarjeta de crédito, con periodo de prueba gratuito transcurrido el cual se factura automáticamente el servicio sin avisar al usuario.
30. *Vid. ult. loc.*, se trata del supuesto en el que un sitio o juego solicita credenciales de un usuario en redes sociales o correo electrónico con un fin "supuestamente benigno" como encontrar amigos que ya emplean el servicio, pero que posteriormente envía mensajes masivos utilizando la cuenta.
31. *Vid. ult. loc.*, se trata de cargos que aparecen a la hora de hacer el pago (como gastos de envío o tasas).
32. *Vid.* BRINGNULL, H., web "Dark Patterns" de 2010, ob. cit., al explicar que "(e)he attention of the user is focused on one thing in order to distract its attention from another".
33. Sobre la configuración y clasificación de patrones oscuros de interfaces engañosos, y el aumento de tipos detectado, en la reciente doctrina, *vid.* LEISER, M., *Illuminating Manipulative Design: from "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive* (April 14, 2022), pp. 1-31. Available at SSRN: https://ssrn.com/abstract=4418586 (fecha de consulta: 5.7.2027). En particular, al afirmar que de los 12 detectados en 2010 se pasa a los 84 identificados en 2019.
34. *Vid.* BRIGNULL, H., LEISER, M., SANTOS, C., & DOSHI, K. (2023, April 25), ob. cit., seguido en este punto: "Comparison prevention; Confirmshaming; Disguised ads; Fake scarcity; Fake social proof; Fake urgency; Forced action; Hard to cancel; Hidden Costs; Hidden subscription; Nagging; Obstruction; Preselection; Sneaking; Trick wording; Visual interference". Para una aproximación a estos patrones oscuros, *vid.* del autor, en CASTELLÓ PASTOR, J. J. (Dir.), *Análisis del reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, ob. cit., pp. 171-200.

(UE) 2022/2065, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales), toda vez que constituye la primera regulación expresa dedicada a los interfaces engañosos[35]. Sin embargo, existen otros instrumentos normativos que regulan los interfaces engañosos, tanto de forma expresa como de forma tácita o implícita, al tutelar diversos intereses que se verán afectados por este tipo de prácticas que toman como base las interfaces de usuarios que resultan engañosos[36].

Un ejemplo ilustrativo del tratamiento heterogéneo de los patrones oscuros en la normativa europea, que ha merecido crítica de algunos sectores de la doctrina, se observa en la propia definición de *"Dark Patterns"*, toda vez que, mientras que algunos instrumentos normativos contienen definiciones expresas, como es de ver en el Reglamento de Servicios Digitales al ofrecer su concepto en el antes citado Cdo. 67 o también en la normativa europea de datos, otras normativas como las correspondientes en materia de protección de datos y prácticas comerciales desleales con consumidores desplazan su definición o mención a las Directrices que explican en detalle aquellos instrumentos normativos. Otras normativas europeas como la referente a los mercados digitales y la relativa a la inteligencia artificial no ofrecen definición alguna[37].

En cualquier caso, bajo la expresión regulación vigente, se indican en este y en los siguientes apartados los principales cuerpos normativos de la Unión Europea en los que de forma expresa o tácita se ordena el fenómeno conocido como *"Dark Patterns"* o patrones oscuros en los interfaces en línea, con el fin de aproximar las diferentes facetas tuteladas, así como las ventajas e inconvenientes de este tipo de regulación, que bien se puede calificar a la fecha de fragmentaria, y que, en última instancia, incide en aspectos tales como la transparencia y protección del consumidor. En este sentido, fue la antes citada Comunicación de la Comisión sobre la Nueva Agenda del Consumidor del año 2020 el primer acto en el que se menciona de forma expresa este fenómeno y en el que se advierte la necesidad de abordarlo, lo que se

35. Reglamento (UE) 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) (DOUE núm. 277, 27.10.2022).

36. *Vid.* GRAEF, I., "The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?" (April 3, 2023). Forthcoming as a book chapter in WOODCOCK, R. A., *Toward an Inframarginal Revolution: Markets as Wealth Distributors*, Cambridge University Press 2023, TILEC Discussion Paper No. 2023-07, Tilburg Law School Research Paper, pp. 16 y 17:

37. *Vid.* HERMAN J., Dark patterns: EU's regulatory efforts. *Security and Privacy*, ob. cit., p. 7.

ha llevado a cabo de diversas maneras en múltiples normativas europeas, y lo que puede ocasionar los problemas derivados de una sobreabundancia normativa como pueden ser la existencia de solapes en la protección y la existencia de dificultades a la hora de determinar la normativa aplicable (o en su caso la hipotética complementariedad entre varias normas), lo que en definitiva puede llevar a restar operatividad al sistema.

Con todo, no se puede olvidar que cada normativa cuenta con unos objetivos e intereses jurídicamente protegidos concretos, un determinado ámbito de aplicación y conjunto de acciones legales y remedios jurídicos específicos. Como ha esquematizado la doctrina internacional[38], la regulación de la protección del consumidor tiene como ámbito la lealtad en las prácticas leales aplicables a consumidores, persigue un daño individual y se activa con carácter *ex post* a nivel nacional, mientras que la regulación de la protección de datos se centra en el procesamiento de datos personas como objeto. Por su parte, el Reglamento de Servicios Digitales se refiere al diseño, organización y gestión de los interfaces en línea de los prestadores de plataformas, que engañen o manipulen a los consumidores y usuarios, lo conlleva en este contexto un daño de carácter colectivo *ex ante* en el ámbito, no nacional, sino de la Unión Europea[39].

En consecuencia, la configuración de la regulación de aplicación a las interfaces engañosas requiere atender a las diferencias que presenta cada instrumento normativo de la Unión Europea, dada la diferente orientación, objeto y finalidad de cada una de llas y, en su caso, articularse a través de diversas normativas llamadas a aplicarse de forma subsidiaria, como es de ver, en relación con el artículo 25 del Reglamento de Servicios Digitales con respecto a la Directiva de Prácticas Comerciales Desleales con Consumidores y del Reglamento General de Protección de Datos[40].

38. *Vid.* GRAEF, I., "The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?" (April 3, 2023). Forthcoming as a book chapter in WOODCOCK, R. A., *Toward an Inframarginal Revolution: Markets as Wealth Distributors*, Cambridge University Press 2023, TILEC Discussion Paper No. 2023-07, Tilburg Law School Research Paper, pp. 16 y 17.

39. *Vid. ult. loc.*, afirma GRAEF que, la normativa sobre Defensa de la competencia europea tiene un alcance que corresponde con los efectos anticompetitivos del abuso de la posición de dominio, que supone un daño colectivo y la protección que brinda se activa en ante en el ámbito de la Unión Europea. Es preciso matizar que en función del alcance de la conducta se apreciaría en el ámbito nacional o de la Unión Europea.

40. Para tal fin se presentan en los siguientes apartados los diversos instrumentos normativos de la Unión Europea. En primer lugar, se aproxima la regulación del RSD por regular en su art. 25, por primera vez de manera expresa a las *"Dark Patterns"*, y, posteriormente, el resto de los instrumentos normativos previos y posteriores al RDS

1. RECONOCIMIENTO DE LOS "PATRONES OSCUROS" EN INTERFACES DE USUARIOS EN LA COMUNICACIÓN SOBRE LA NUEVA AGENDA DEL CONSUMIDOR DE 2020

El primer acto expreso de la Unión Europea en el que se refleja el fenómeno de las interfaces engañosos fue la Comunicación de la Comisión Europea, "Nueva Agenda del Consumidor Reforzar la resiliencia del consumidor para una recuperación sostenible"[41], en la que se describen como ámbitos principales la transición ecológica y también la transición digital. Como se expresa en la Comunicación, la transición digital está cambiando de forma radical las vidas de los consumidores, en el sentido de ofrecerles más oportunidades y una mayor variedad de bienes y servicios. En este contexto en el que se expresa que "(d)eben abordarse las prácticas comerciales que pasan por alto el derecho de los consumidores a tomar decisiones informadas, hacen un uso fraudulento de sus sesgos de comportamiento o distorsionan sus procesos de toma de decisiones. Estas prácticas incluyen el uso de patrones 'oscuros', determinadas prácticas de personalización que a menudo se basan en la elaboración de perfiles, la publicidad encubierta, el fraude, la información falsa o engañosa y los comentarios manipulados de consumidores. Se requieren orientaciones adicionales sobre la aplicabilidad de los instrumentos de Derecho en materia de protección de los consumidores, tales como la Directiva sobre las prácticas comerciales desleales y la Directiva sobre los derechos de los consumidores, a estas prácticas. En última instancia, los consumidores deben gozar de un nivel de protección y equidad en línea comparable al que tienen fuera de línea"[42]. A estos efectos, como se

---

llamados a regular también las interfaces engañosas, que se presentarán siguiendo un orden cronológico.

41. Comunicación de la Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Nueva Agenda del Consumidor Reforzar la resiliencia del consumidor para una recuperación sostenible, Bruselas, 13.11.2020 COM (2020) 696 final.

42. *Ibid.*, pp. 11 y 12. A estos efectos, se indica el diferente ámbito, objeto y tutela de instrumentos normativos ya aprobados en la actualidad. En este sentido, GRAEF expresó un conjunto de consideraciones en 2023 sobre propuestas normativas en esa fecha, pero que bien continúan teniendo vigencia,. En concreto, que la Propuesta de Reglamento sobre Inteligencia Artificial se centra en la comercialización, puesta en servicio o utilización de un sistema de inteligencia artificial y el despliegue de técnicas subliminales, toma en consideración el daño individual y se trata de una protección *ex ante* a nivel nacional. Asimismo, que la Propuesta de Ley de Datos, comparte el foco en el daño individual con carácter *ex ante* en el ámbito nacional, pero se centra en la recepción de datos del usuario a terceros y en la coacción, engaño o manipulación a los usuarios perjudicando su autonomía y toma de decisiones. *Vid.*, BRENNCKE, M., "Regulating dark patterns", *Notre dame J. Int'L & Comp. L.* Vol. XIV: I, p. 16, al apreciar que la teoría normativa adoptada por el Derecho de consumo de la Unión Europea es la autonomía.

indica en la citada Comunicación de 2020 la referencia a los patrones oscuros incide en los "(d)iseños de interfaces de usuario que tienen la finalidad de manipular a los consumidores".

Esta será la finalidad que marcará la constante en la definición, caracterización y regulación de los interfaces engañosos: la finalidad de manipular a los consumidores. Con todo, de la lectura de la comunicación de 2020 cabe deducir el interés del consumidor como aspecto principal en la ordenación de los patrones oscuros. En este sentido, tampoco puede pasar inadvertido el llamamiento a las normativas europeas contenidas en las directivas sobre prácticas comerciales desleales y derechos de los consumidores, así como en general a las prácticas comerciales en general que no respeten los derechos de los consumidores, lo que ciertamente puede exceder de los patrones oscuros en el ámbito digital y alcanzar a otro tipo de prácticas en el contexto digital. Es en estos nuevos escenarios donde tal vez la futura normativa denominada *Digital Fairness Act* esté llamada a desplegar también su ámbito de aplicación.

2. REGLAMENTO DE SERVICIOS DIGITALES DE 2022 COMO PRIMERA REGULACIÓN EXPRESA DE LAS INTERFACES ENGAÑOSAS EN LA UNIÓN EUROPEA

Sin perjuicio de la preexistencia normativas europeas susceptibles de aplicación al fenómeno de los patrones oscuros, sin mencionarlos expresamente (por consistir en conductas que se incardinan en el ámbito de aplicación de dichas normas), fue el Reglamento de Servicios Digitales de 2022 el instrumento normativo qué me ofreció la primera regulación expresa de las interfaces engañosas o patrones oscuros. En concreto, es el artículo 25 del reglamento de servicios digitales el precepto que establece la prohibición del diseño, organización y gestión de interfaces en línea que constituyan patrones oscuros por engañar o manipular a sus destinatarios o por distorsionar u obstaculizar sustancialmente su capacidad de tomar decisiones de una manera libre e informada[43].

Bajo el título "(d)iseño y organización de interfaces en línea" el artículo 25 establece la mencionada prohibición, al tiempo que su inaplicación a las

43. Art. 25.1 RSD: "1. Los prestadores de plataformas en línea no diseñarán, organizarán ni gestionarán sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas".

prácticas contempladas en la directiva de prácticas comerciales desleales o en el Reglamento General de Protección de Datos[44]. No cabe duda que la articulación de esta protección subsidiaria a la prevista en aquellas normas previas plantea diversas dudas sobre los contornos del ámbito de aplicación de cada norma y, en lo que más puede interesar, en su eficacia a la hora de preservar los derechos de los consumidores y usuarios. En cualquier caso, como se verá en siguientes apartados, es necesario acotar debidamente el ámbito de aplicación de cada norma y el objeto de protección concreto de cada una de ellas para así minimizar los posibles solapes entre las mismas de mayor coherencia. Finalmente, el artículo 25 del Reglamento de Servicios Digitales contempla la posibilidad de que la comisión pueda publicar directrices sobre la aplicación de la prohibición a los prestadores de plataformas en línea de diseño organización y gestión de interfaces en línea que constituyan patrones oscuros. En este puntose ofrecen, en particular, algunas prácticas específicas cómo son las consistentes en la preminencia de algunas opciones que se presentan al consumidor o usuario, la solicitud reiterada de una misma elección y la dificultad a la hora de finalizar una suscripción[45].

Al respecto cabe afirmar que si bien debe ser bienvenida la posibilidad de que la comisión publique directrices sobre la aplicación del artículo 25.1 a prácticas específicas, también es oportuno comentar que también lo hubiera sido contemplar la posibilidad de que la Comisión pueda publicar directrices sobre cómo el apartado 2 del artículo 25 del Reglamento de Servicios Digitales debe cohesionarse con las normativas europeas en materia de prácticas comerciales desleales y de protección de datos citadas expresamente. Pero también y a la vista de las normativas europeas llamadas a regular los patrones oscuros aparecidas en los últimos años para ofrecer orientación de cómo se deben cohesionar, en general, con la protección y tutela prevista en el artículo 25 del Reglamento de Servicios Digitales.

La Directiva de Servicios Digitales Presenta la virtud de ofrecer la definición de interfaces en línea antes mencionada, al igual que una definición y caracterización de las interfaces engañosas coma de las plataformas en línea

44. Art. 25.2 RSD: "2. La prohibición del apartado 1 no se aplicará a las prácticas contempladas en la Directiva 2005/29/CE o en el Reglamento (UE) 2016/679".

45. Art. 25.3 RSD: "3. La Comisión podrá publicar directrices sobre cómo el apartado 1 se aplica a prácticas específicas, en particular: a) dar más protagonismo a determinadas opciones al pedir al destinatario del servicio que tome una decisión; b) solicitar reiteradamente que el destinatario del servicio elija una opción cuando ya se haya hecho esa elección, especialmente a través de la presentación de ventanas emergentes que interfieran en la experiencia del usuario; c) hacer que el procedimiento para poner fin a un servicio sea más difícil que suscribirse a él".

que sirven para justificar su prohibición. En particular, el Cdo. 67 define las interfaces engañosas, en el contexto de las plataformas en línea, cómo "prácticas que distorsionan o merman sustancialmente, de forma deliberada o efectiva, la capacidad de los destinatarios del servicio de tomar decisiones autónomas y con conocimiento de causa". De esta manera, un patrón oscuro se puede definir en esencia como una interfaz engañosa. El engaño deriva de las prácticas que causan a través de la interfaz engañosa la distorsión o merma sustancial de la capacidad del destinatario o usuario de tomar decisiones autónomas y fundadas. A continuación, el citado Cdo. 67 advierte que estas prácticas pueden ser utilizadas para persuadir a los destinatarios de que adopten comportamientos o decisiones que no desean, qué conllevan consecuencias negativas para ellos. Es en este aspecto en el que el legislador europeo justifica la prohibición a los prestadores de plataformas en línea de engañar o "empujar" en esta dirección a los destinatarios "y distorsionar u obstaculizar la autonomía, la toma de decisiones o la capacidad de elección de los destinatarios del servicio a través de la estructura, el diseño o las funcionalidades de una interfaz en línea o una parte de esta".

Asimismo, este apartado del Cdo. de Reglamento de Servicios Digitales pone de manifiesto un conjunto de prácticas constitutivas de patrones oscuros, *"entre otras"*, lo que asienta no un sistema de *numerus clausus*, sino un sistema de *numerus apertus*, capaz de dar cabida a futuras realidades no conocidas a la fecha que sean un fruto del incesante avance tecnológico. Dichas prácticas constitutivas de patrones oscuros se caracterizan en el Cdo. 67 en la existencia de un diseño abusivo que no favorecerá los intereses de los destinatarios, aprovechando la falta de neutralidad en la presentación de las opciones que deberán recibir diferentes sentidos de la persona como la vista o la audición sobre la que la persona tomará una decisión[46]. Otras prácticas que a juicio del legislador europeo también deben merecer la consideración de interfaces engañosas y en consecuencia patrones oscuros, en este contexto, son las consistentes en solicitar al destinatario de manera reiterada que tome una decisión que ya tomó, la consistente en dificultar la anulación

46. Cdo. 67 RSD: "Por esta razón, debe prohibirse a los prestadores de plataformas en línea engañar o empujar en esta dirección a los destinatarios del servicio y distorsionar u obstaculizar la autonomía, la toma de decisiones o la capacidad de elección de los destinatarios del servicio a través de la estructura, el diseño o las funcionalidades de una interfaz en línea o una parte de esta. Entre estas prácticas se han de incluir, entre otras, las opciones de diseño abusivas que dirigen al destinatario hacia acciones que benefician al prestador de plataformas en línea, pero que pueden no favorecer los intereses de los destinatarios, al presentar opciones de una manera que no es neutra, por ejemplo, dando más protagonismo a determinadas opciones mediante componentes visuales, auditivos o de otro tipo, cuando se le pide al destinatario del servicio que tome una decisión".

de un servicio de forma desproporcionada con respecto a la suscripción al mismo, la de dificultar diversas opciones, la de dificultar excesivamente la interrupción de compras o la desconexión de una plataforma en línea[47], así como engañar a los destinatarios para que tomen decisiones sobre transacciones o ajustes por defecto que posteriormente se revelarán difíciles de modificar, lo que distorsionará y mermará su autonomía así como su toma de decisiones y capacidad de elección[48].

Por otra parte, el Cdo. 67 del Reglamento de Servicios Digitales reconoce la existencia de un espacio de interacción directa entre prestador y destinatario al aclarar que "las normas contra las interfaces engañosas no deben entenderse en el sentido de que impidan a los prestadores interactuar directamente con los destinatarios del servicio y ofrecerles servicios nuevos o adicionales", toda vez que existen prácticas legítimas, como las publicitarias, que sean conformes con el Derecho de la Unión y que "no deben considerarse en sí mismas interfaces engañosas". Finalmente, en este punto el Reglamento de Servicios Digitales aprecia que dichas normas represoras de las interfaces engañosas "deben interpretarse en el sentido de que se aplican a las prácticas prohibidas que entran en el ámbito de aplicación del presente Reglamento en la medida en que no estén ya cubiertas por la Directiva 2005/29/CE o el Reglamento (UE) 2016/679". Con ello se explica que la prohibición de patrones oscuros del Reglamento de Servicios Digitales solo se aplicará a las interfaces engañosas que entren dentro del ámbito de aplicación de la norma con carácter subsidiario a la aplicación de la normativa contenida en la Directiva de Prácticas Desleales con Consumidores y el Reglamento General de Protección de Datos.

2.1. Ámbito de aplicación

La revisión, siquiera sucinta, del ámbito de aplicación del artículo 25 del Reglamento de Servicios Digitales resulta necesaria para determinar la forma en que deberá articularse con las normativas europeas sobre prácticas desleales y protección de datos llamadas a aplicarse de forma preeminente y que, en lo que ahora interesa, constituyen una parte de la regulación de

47. *Vid. ult. loc.*, en concreto: "(…) dificultar excesivamente la interrupción de las compras o la desconexión de una plataforma en línea determinada que permite a los consumidores celebrar contratos a distancia con comerciantes, y engañar a los destinatarios del servicio empujándoles a tomar decisiones sobre transacciones o mediante ajustes por defecto que sean muy difíciles de cambiar, dirigiendo de forma injustificada la toma de decisiones del destinatario del servicio (…)".

48. *Vid. ult. loc.*

las interfaces engañosas, aun de forma tácita, pero anterior en el tiempo al Reglamento de Servicios Digitales. Este hecho justifica que se preste mayor atención al ámbito de aplicación de las normativas relacionadas en el artículo 25.2 del Reglamento de Servicios Digitales. Desde una perspectiva subjetiva, los destinatarios de la prohibición del artículo 25.1 son los prestadores de plataformas en línea, lo que difiere ya no solo de los destinatarios previstos en las otras normativas citadas expresamente en el artículo 25.2 del Reglamento de Servicios Digitales[49], sino también del correspondiente al propio Reglamento de Servicios Digitales, toda vez que la prohibición de interfaces engañosas del art. 25.1 del Reglamento de Servicios Digitales solo se aplica a plataformas en línea[50] y no a otras entidades a las que se aplica el Reglamento de Servicios Digitales, por lo que no se aplicará a otros agentes que empleen patrones oscuros que no sean considerados "plataformas en línea" por no cumplir los criterio requeridos para ello en el contexto del Reglamento de Servicios Digitales[51]. Además, de acuerdo con el artículo 19 del citado Reglamento, se excluyen las microempresas y pequeñas empresas, salvo que se trate de prestadores de plataformas en línea de gran tamaño[52].

Desde una perspectiva objetiva, y de acuerdo con el tenor literal del artículo 25 del Reglamento de Servicios Digitales, se establece la prohibición de diseñar, organizar y gestionar interfaces en línea que engañen, manipulen, distorsionen u obstaculicen sustancialmente de otro modo la capacidad de tomar decisiones libres e informadas por parte de los destinatarios. Sin embargo, como ha apreciado la doctrina internacional[53], no se precisa la

49. Valga como ejemplo el art. 3.1 DPCD: "La presente Directiva será aplicable a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores según establece el artículo 5, antes, durante y después de una transacción comercial en relación con un producto".

50. *Vid.* LEISER, M. and SANTOS, C., *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface*, ob. cit., pp. 20 y 21.

51. *Vid. ult. loc.*, sobre el caso de juegos *online* como plataformas en línea, lo que se ejemplifica con supuesto del juego "Candy Crush", para el que la noción de plataforma en línea puede resultar ambigua.

52. En concreto, de acuerdo con el art. 19 del Reglamento de Servicios Digitales, la Sección 3.ª del Capítulo III del Reglamento de Servicios Digitales (Salvo el art. 24.3 RSD), sobre disposiciones adicionales aplicables a los prestadores de plataformas en línea (en el que se ubica el art. 25) no se aplicará a los prestadores de plataformas en línea que sean microempresas o pequeñas empresas, conforme a la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO 20.5.2003 L 124)), pero sí a prestadores de plataformas en línea de gran tamaño, incluso si se trata de microempresas o pequeñas empresas (art. 19.2 y 3 RSD).

53. *Vid.* LEISER, M. and SANTOS, C., *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface*, ob. cit., p. 21. También se ha apreciado

prohibición con respecto a cada tipo de influencia lo que puede dar lugar a interpretaciones divergentes y, en consecuencia, inseguridad jurídica.

2.2. Articulación con la Directiva de Prácticas Comerciales Desleales con Consumidores y del Reglamento General de Protección de Datos

Finalmente, el artículo 25.2 del Reglamento de Servicios Digitales establece límites al ámbito de aplicación del artículo 25.1 del citado Reglamento, al declarar la prevalencia de la Directiva de Prácticas Comerciales Desleales con Consumidores y del Reglamento General de Protección de Datos y la aplicación subsidiaria del artículo 25.1 del Reglamento de Servicios Digitales, lo que supone que la prohibición de las interfaces engañosas establecida en el artículo 25.1 del Reglamento de Servicios Digitales no se aplica a las conductas prohibidas ya por aquellos cuerpos normativos europeos en materia de prácticas comerciales desleales y de datos. Esta articulación entre protecciones ha generado dudas sobre la eficacia del artículo 25 del Reglamento de Servicios Digitales en la mayoría de patrones oscuros podrán verse afectadas por las normativas citadas de prácticas comerciales desleales y datos[54]. Por otra parte, también se ha incidido en que la naturaleza subsidiaria del Reglamento de Servicios Digitales posibilitaría que algunos patrones oscuros o interfaces engañosos no estuvieran cubiertos por la legislación existente, al igual que los patrones oscuros de próxima generación que alcanzan al metaverso, así como en la necesidad de ahondar en el concepto y caracterización las interfaces engañosas[55].

3. DIRECTIVA SOBRE LAS PRÁCTICAS COMERCIALES DESLEALES DE 2005

La Directiva de Prácticas Comerciales Desleales con Consumidores de 2005 no regula expresamente las interfaces engañosas, sin embargo, resulta de aplicación en la medida en que los patrones oscuros concretos pueden constituir prácticas comerciales desleales de las previstas en el ámbito del

---

los autores que esta disposición general podría interpretarse como una disposición anticipatoria relacionada con las tecnologías emergentes y nuevos formas de influencia que incidan en el comportamiento del usuario.

54. *Vid. ult. loc*. Cfr. *Vid.* GRAEF, I., "The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?", ob. cit., p. 7, al apreciar que solo un conjunto limitado de patrones oscuros entrará dentro del alcance de las prohibiciones específicas, por lo que es necesario un análisis caso por caso para determinar si una interfaz debe considerarse desleal.

55. *Vid.* LEISER, M. and SANTOS, C., Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface, ob. cit., p. 21.

artículo 5 sobre prácticas contrarias a la diligencia profesional, del artículo 6 y 7 con respecto a las prácticas engañosas o inclusive como prácticas agresivas previstas en el artículo 8 de la Directiva de Prácticas Comerciales Desleales. Por otra parte, cabe recordar la remisión expresa que efectúa el artículo 25.2 del Reglamento de Servicios Digitales, sin perjuicio del diverso ámbito de aplicación de cada normativa, antes visto.

En cualquier caso, las dudas con respecto a la aplicación y articulación de la Directiva de Prácticas Comerciales Desleales a los patrones oscuros quedaban ya disipadas por la Comunicación de la Comisión titulada "Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior" del año 2021[56], en la que al incidir en las prácticas de manipulación introduce el término "patrón oscuro" como un tipo de estímulo malintencionado, incorporado en las interfaces digitales, si bien, como se advierte en las Directrices de 2021, el término "patrón oscuro" no tiene una definición jurídica en la Directiva. No obstante, como pone de manifiesto la Guía de 2021, la Directiva de Prácticas Comerciales Desleales se aplicará a cualquier práctica comercial desleal siempre y cuando se cumplan los requisitos del ámbito de aplicación material de esta Directiva[57], lo que se debe apreciar de forma independiente de su clasificación. Esta aproximación debe saludarse de manera positiva dada su coherencia y operatividad, pues se centra la atención en el carácter desleal de la conducta más allá del medio o soporte en el que se lleva a cabo. Por otra parte, como explica la Guía de 2021, "los patrones oscuros podrían basarse en datos y personalizarse, o aplicarse de general cuando se aprovechan los sesgos heurísticos y conductuales, como los derivados de la 'escasez'"[58]. Finalmente, en lo que ahora interesa, fue la Guía de 2021 la que aclaró que la Directiva de Prácticas Comerciales Desleales "puede utilizarse para cuestionar la equidad de tales prácticas" consistentes en aplica patrones oscuros en las relaciones comerciales entre empresas y consumidores, y ello sin perjuicio de otros instrumentos legales de la Unión Europea, para lo que se cita expresamente el Reglamento General para la Protección de Datos[59]. Tras todo lo dicho, cabe concluir

56. *Vid.* Comunicación de la comisión, "Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior" DOUE 29.12.2021 C 526/1 (en adelante "Guía de 2021"), pp. 1-129 (en particular, pp. 99 y ss.).
57. *Ibid.*, p. 101.
58. *Ibid.*, p. 102.
59. *Vid. ult. loc.*

que la determinación de la normativa aplicable de la Unión Europea a una determinada interfaz engañosa, que constituya un patrón oscuro, requerirá su análisis caso a caso como se dijo anteriormente[60] y deberá atender a diversos criterios como el referente al ámbito material afectado, como bien puede ser el correspondiente a las prácticas comerciales desleales o a la protección de datos, y, posteriormente, al referente a los destinatarios de las normas, que en el caso de las prácticas comerciales desleales con consumidores quedará circunscrito a las relaciones comerciales entre empresas y consumidores[61]. Verificados estos extremos se deberá examinar el encaje de la conducta concreta identificada en el patrón oscuro para determinar si resulta de aplicación la Directiva de Prácticas Comerciales Desleales o, en su caso y con carácter subsidiario, el artículo 25 del Reglamento de Servicios Digitales, siempre y cuando se observen también los requisitos previstos para su aplicación.

4. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE 2016

El Reglamento General de Protección de Datos es el otro instrumento normativo de la Unión Europea frente al que cede la aplicación del Reglamento de Servicios Digitales en virtud del artículo 25.2 de este último. En lo que ahora interesa, el Reglamento General de Protección de Datos no menciona expresamente a las interfaces engañosas, pero sí que incide en las mismas al ofrecer tutela y protección sobre el consentimiento. En concreto, ahonda en el "consentimiento" al definir en su artículo 4.11) el "consentimiento del interesado" como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". De la lectura de esta definición se advierte con facilidad que las *"Dark Patterns"* subvertirán los elementos configuradores del consentimiento del interesado, al afectar mediante manipulación el carácter libre de la declaración por la que se acepta por una persona el tratamiento de datos personales. De esta forma, pese a que el Reglamento General de

60. *Vid.* GRAEF, I., "The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?", ob. cit., p. 7.

61. La Guía de 2021 (pp. 101 y 102) incluye algunos patrones oscuros en algunas conductas expresamente prohibidas en cualquier circunstancia en el Anexo I de la DPCD, como las de "señuelo y cambio", las que buscan crear sensación de urgencia por la disponibilidad de un producto durante un tiempo muy limitado y que deviene falso, las que proporcionan información sobre condiciones del mercado que no son exactas, así como "afirmar que el consumidor ha ganado un premio, sin concederlos ni algo razonablemente equivalente" y la persistencia. Algunas prácticas de los arts. 6 y 7 DPCD se consideran "patrones oscuros" como las pruebas gratuitas engañosas y las trampas de suscripción.

Datos no se refiere expresamente a las interfaces engañosas sí que es fácil entender que dichas prácticas manipulan y merman el consentimiento en los términos del art. 4.11) Reglamento General de Protección de Datos.

No obstante, cualquier duda al respecto quedó disipada por las "Directrices 03/2022 sobre patrones de diseño engañosos en las interfaces de plataformas de medios sociales: cómo reconocerlos y evitarlos" en su versión de 14 de febrero de 2023[62] en la que se afirma que "(l)os patrones de diseño engañosos tienen por objeto influir en el comportamiento de los usuarios y pueden obstaculizar su capacidad para proteger eficazmente sus datos personales y tomar decisiones conscientes", por lo que "(l)as autoridades de protección de datos son responsables de sancionar el uso de patrones de diseño engañosos si estos incumplen los requisitos del RGPD"[63]. En consecuencia, se recogen[64] varias categorías de *"Dark Patterns"* específicas del ámbito de la protección de datos[65], como son las conocidas[66] como *"Overloading"*, que se relaciona con la presentación de demasiadas opciones; *"Skipping"* que supone el diseño de una determinada interfaz de manera que el usuario se olvida o no repara en los datos; *"Stirring"* por el que se afecta a la elección del usuario apelando a sus emociones a través de la interfaz; *"Obstructing"* por el que bloquear a los usuarios en el proceso de información en materia de protección de datos; *"Fickle"* que acontece cuando el diseño de una interfaz no es claro y dificulta la navegación en materia de datos; y, asimismo, el denominado *"Left in the dark"* que incide en el supuesto de las interfaces cuyo diseño oculta información o herramientas control de datos.

---

62. *Vid.* EUROPEAN DATA PROTECTION BOARD, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and) avoid them*, Version 2.0 Adopted on 14 February 2023, pp. 1-82 (en adelante, "Directrices de 2023").
63. *Ibid.*, p. 3.
64. *Ibid.*, p. 8, al explicar que el objetivo de las Directrices de 2023, "es ofrecer recomendaciones y orientaciones para el diseño de las interfaces de las plataformas de redes sociales. A los efectos de estas Directrices, por redes sociales se entienden las plataformas en línea que permiten el desarrollo de redes y comunidades de usuarios entre los que se comparte información y contenidos".
65. *Ibid.*, p. 3 al definir los "patrones de diseño engañosos", que son los que "se consideran interfaces y experiencias de usuario implementados en plataformas de redes sociales que intentan influir en los usuarios para que tomen decisiones no deseadas, involuntarias y potencialmente perjudiciales, a menudo hacia una decisión contraria al interés superior de los usuarios y en favor de los intereses de las plataformas de redes sociales, en relación con el tratamiento de sus datos personales"
66. *Vid.* portal web de la Agencia Española de Protección de Datos (AEPD), Entrada "Dark patterns: Manipulación en los servicios de Internet", de 19.5.2022 (disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet) (última consulta: 7-2025).

Desde la perspectiva del Reglamento General de Protección de Datos, el consentimiento del interesado se preserva en la regulación que ofrece el citado Reglamento en materia de principios relativos al tratamiento, en su artículo 5.1, en la medida en que los datos personales serán "tratados de manera lícita, leal y transparente en relación con el interesado ('licitud, lealtad y transparencia')". Interesa destacar que el artículo 5.2 del Reglamento General de Protección de Datos establece la denominada "responsabilidad proactiva del responsable del tratamiento", toda vez que también lo será "del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo". En consecuencia, de nuevo, es fácil advertir que los *"Dark Patterns"* contravendrán los principios de licitud, lealtad y transparencia que deben presidir el tratamiento de datos, lo que requiere la responsabilidad proactiva del responsable de dicho tratamiento. Además, el artículo 7 del Reglamento, al regular las condiciones para el consentimiento, también atribuye al responsable del tratamiento el deber "ser capaz de demostrar" que el interesado consintió el tratamiento de sus datos personales[67]. Finalmente, las interfaces engañosas también afectarán a la regulación sobre transparencia de la información y las modalidades de ejercicio del interesado, en los términos previstos en el artículo 12.1 del Reglamento General de Protección de datos. En este precepto, se establece la obligación del responsable del tratamiento de tomar las medidas oportunas para facilitar al interesado toda información[68], así como cualquier comunicación relativa al tratamiento[69], que se deberá realizar en lo que ahora interesa "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño"[70]. En consecuencia, el empleo de interfaces engañosas que afecten a la concisión de la información sobre tratamiento de datos, a su transparencia, entendimiento, accesibilidad, claridad y sencillez, supondrán un incumplimiento del artículo 12.1 del Reglamento General de Protección de Datos. Finalmente, la protección frente a las *"Dark Patterns"* también se aprecia en la regulación establecida en el artículo 25 del Reglamento sobre la protección de datos desde el diseño y por defecto[71].

---

67. Art. 7.1 RGPD.
68. Prevista en los arts. 13 y 14 RGPD.
69. Recogida en los arts. 15 a 22 y 34 RGPD.
70. Sigue el art. 12.1 RDPG: "La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios".
71. *Vid.* Directrices de 2023, p. 12, al explicar que además la disposición sobre lealtad del tratamiento del art. 5 RDPD, "los principios de responsabilidad proactiva, transpa-

5. REGLAMENTO DE MERCADOS DIGITALES DE 2022

El Reglamento de Mercados Digitales forma parte del paquete lanzado por el legislador europeo en el año 2022 junto con el Reglamento de Servicios Digitales. En concreto, el Reglamento de Mercados Digitales está orientado[72] a la prevención de prácticas anticompetitivas y en este sentido impone un conjunto de obligaciones a grandes plataformas como "guardián de acceso" o *"gatekeepers"*[73]. Esta precisión resulta relevante en la determinación del ámbito de aplicación de la norma desde la perspectiva subjetiva. Este instrumento normativo de la Unión Europea no contiende referencia expresa a las *"Dark Patterns"*, pero sí que debe cubrirlas en relación con el consentimiento[74].

Como explica[75] el Cdo. 37 del Reglamento de Mercados Digitales sobre la "alternativa menos personalizada", esta no debe ser diferente ni con una calidad "degradada" con respecto al servicio que se presta a los usuarios finales que sí que prestaron su consentimiento, y en este contexto afirma que "(n)o prestar el consentimiento no debe ser más difícil que prestarlo" y que cuando se solicite el consentimiento, se debe presentar "proactivamente

---

rencia y obligación de protección de datos desde el diseño establecidos en el artículo 25 del RGPD también son pertinentes en lo que respecta al marco del diseño, y los patrones de diseño engañosos podrían infringir dichas disposiciones".

72. Cfr. art. 1.1 RMD: "La finalidad del presente Reglamento es contribuir al correcto funcionamiento del mercado interior estableciendo normas armonizadas que garanticen a todas las empresas, en toda la Unión, la equidad y la disputabilidad de los mercados en el sector digital donde haya guardianes de acceso, en beneficio de los usuarios profesionales y los usuarios finales".

73. El art. 2.1 RMD define esta figura como "una empresa prestadora de servicios básicos de plataforma, designada de conformidad con el artículo 3" del RMD, lo que acontece de acuerdo con citado art. 3 RMD cuando "a) tiene una gran influencia en el mercado interior; b) presta un servicio básico de plataforma que es una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales, y c) tiene una posición afianzada y duradera, por lo que respecta a sus operaciones, o es previsible que alcance dicha posición en un futuro próximo".

74. Cfr. Arts. 6 a 8 RMD.

75. Previamente, el Cdo. 36 RMD explica que para que los guardianes de acceso no menoscaben deslealmente la disputabilidad de los servicios básicos de plataforma, deben permitir que los usuarios finales puedan elegir libremente participar las prácticas de tratamiento de datos e inicio de sesión ofreciendo una alternativa menos personalizada, pero equivalente, sin que se condicione el uso del servicio básico de plataforma o de algunas funcionalidades al consentimiento del usuario final. En lo que ahora interesa, también expresa que no debe afectar al tratamiento de datos personales o al inicio de sesión de usuarios finales en un servicio por parte del guardián de acceso, con fundamento en la base jurídica del artículo 6, apartado 1, letras c), d) y e), del Reglamento General de Protección de Datos, pero no en el artículo 6, apartado 1, letras b) y f).

al usuario final una solución fácil de usar para que este preste, modifique o retire el consentimiento de manera expresa, clara y sencilla", para lo que se detalla que el consentimiento se presentará a través de "una clara acción afirmativa o declaración que establezca una manifestación de acuerdo libre, específica, informada e inequívoca por parte del usuario final" y que en el momento de prestar el consentimiento, cuando proceda, debe informarse que no prestar el consentimiento puede dar lugar a una oferta menos personalizada, sin que el servicio básico se altere o se vaya a suprimir ninguna funcionalidad. En este contexto, el Cdo. 37 del Reglamento de Mercados Digitales *in fine*, declara que debe ser igual de fácil prestar el consentimiento como retirarlo, por lo que "(los guardianes de acceso no deben diseñar, organizar ni explotar sus interfaces en línea de forma que engañen o manipulen a los usuarios finales o reduzcan o distorsionen de otro modo de manera sustancial su capacidad de prestar su consentimiento libremente". Por ello, en concreto, no debe permitirse que los guardianes de acceso inciten a los usuarios finales más de una vez al año a prestar su consentimiento para el mismo fin de tratamiento respecto del cual inicialmente no dieron su consentimiento o lo retiraron, lo que se prevé en el artículo 5.2 *in fine* del Reglamento de Mercados Digitales[76]. A estos efectos, el Cdo. 37 aclara que el Reglamento de Mercados Digitales *"se entiende sin perjuicio"* de lo dispuesto en el Reglamento General de Protección de Datos. De esta forma se articula la relación entre ambos instrumentos normativos, de manera similar a la prevista en sede del artículo 25 del Reglamento de Servicios Digitales.

Finalmente, también se considera oportuno recordar que el artículo 13 del Reglamento de Mercados Digitales, sobre la "antielusión", establece en su apartado cuarto que los *"gatekeepers"* no incurrirán en ningún comportamiento que menoscabe el cumplimiento eficaz de las obligaciones de los artículos 5 a 7, "con independencia de que ese comportamiento sea contractual, comercial, técnico o de cualquier otra naturaleza, o consista en el recurso a técnicas basadas en el comportamiento o al diseño de interfaces", aspecto este último que bien parece incidir en el empleo de interfaces engañosas.

6. REGLAMENTO DE DATOS DE 2023

El Reglamento (UE) 2023/2854 de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, garantiza que

76. En concreto, el art. 5.2. *in fine* RMD establece: "Cuando el usuario final haya denegado o retirado el consentimiento prestado a los fines del párrafo primero, el guardián de acceso no solicitará el consentimiento para el mismo fin más de una vez en el plazo de un año."

los usuarios de un producto conectado o servicio relacionado en la Unión puedan acceder a los datos generados por el uso de dicho producto conectado[77]. Su objeto se centra en la puesta a disposición de datos y otros aspectos relacionados[78]. En lo que interesa, el Reglamento de Datos de 2023 expone el tratamiento de las interfaces engañosas en su Cdo. 38 al introducir el principio de minimización de datos, sin dificultar el ejercicio de opciones y derechos de los usuarios que regula en el artículo 6 el Reglamento de Datos.

En concreto, el Cdo. 38 del Reglamento de Datos explica que el tercero, una vez reciba acceso de los datos debe tratarlos para el fin acordado con el usuario "sin injerencia del titular de datos", y es en este contexto en el que se explica que "(p)ara el usuario debe ser tan fácil denegar o interrumpir el acceso del tercero a los datos como autorizarlo. Ni los terceros ni los titulares de datos deben dificultar indebidamente el ejercicio de las opciones o los derechos de los usuarios, tampoco ofreciendo opciones a los usuarios de manera no neutra, o coaccionándolos, engañándolos o manipulándolos de algún modo, o neutralizando o mermando su autonomía, toma de decisiones u opciones, tampoco a través de una interfaz digital de usuario o de una parte de ella. En ese contexto, los terceros o los titulares de datos no deben basarse en los denominados 'patrones oscuros' (elementos engañosos) a la hora de diseñar sus interfaces digitales"[79]. Por lo tanto, los terceros o los titulares de datos no deben basarse en los denominados "patrones oscu-

77. Cdo. 5 RD.

78. Art. 1.1 RDM: "Objeto y ámbito de aplicación. 1. El presente Reglamento establece normas armonizadas sobre lo siguiente, entre otros: a) la puesta a disposición de datos de productos y de datos de servicios relacionados en favor de los usuarios del producto conectado o servicio relacionado; b) la puesta a disposición de datos por parte de los titulares de datos en favor de los destinatarios de datos; c) la puesta a disposición de datos por parte de los titulares de datos en favor de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión, cuando exista una necesidad excepcional de disponer de dichos datos para el desempeño de alguna tarea específica realizada en interés público; d) la facilitación del cambio entre servicios de tratamiento de datos; e) la introducción de salvaguardias contra el acceso ilícito de terceros a los datos no personales, y f) el desarrollo de normas de interoperabilidad para el acceso, la transferencia y la utilización de datos".

79. Además, el Cdo. 38 ofrece la definición de "patrones oscuros" en el ámbito del RD, al explicar que "son técnicas de diseño que impulsan o engañan a los consumidores para que tomen decisiones que conllevan consecuencias negativas para sí mismos. Estas técnicas de manipulación pueden utilizarse para persuadir a los usuarios, en particular, a los consumidores vulnerables, de que adopten comportamientos que estos no desean, y para engañarlos induciéndoles a tomar decisiones sobre transacciones de divulgación de datos o para influir injustificadamente en la toma de decisiones de los usuarios del servicio, de tal manera que se neutralice o merme su autonomía, su toma de decisiones y su capacidad de elegir entre distintas opciones".

ros" en el diseño sus interfaces digitales para engañarlos induciéndoles a tomar decisiones sobre transacciones de divulgación de datos o para influir injustificadamente en la toma de decisiones de los usuarios del servicio. Sin embargo, como también explica el Cdo. 38 del Reglamento de Datos, las prácticas comerciales habituales y legítimas que sean conformes con el Derecho de la Unión no deben considerarse por sí mismas "patrones oscuros".

Dentro del Capítulo II del Reglamento de Datos, dedicado a la regulación del intercambio de datos de empresa a consumidor y de empresa a empresa, el artículo 4 estable los "Derechos y obligaciones de los usuarios y titulares de datos respecto del acceso, utilización y puesta a disposición de los datos de productos y de los datos de servicios relacionados". Este precepto prevé la obligación de los titulares de datos consistente en no impedir el ejercicio de las opciones o derechos de los usuarios "también ofreciendo opciones a los usuarios de manera no neutra o neutralizando o mermando la autonomía, la toma de decisiones o las opciones del usuario a través de la estructura, el diseño, la función o el modo de funcionamiento de la interfaz digital de usuario o de una parte de ella"[80]. Por otra parte, similar redacción se encuentra en el artículo 6 del Reglamento de Datos al establecer las obligaciones de terceros que reciben datos a petición del usuario, toda vez que contempla la consistente obligación consistente en que el tercero no podrá "dificultar indebidamente el ejercicio de las opciones o los derechos de los usuarios"[81], "tampoco ofreciendo opciones a los usuarios de manera no neutra o coaccionándolos, engañándolos o manipulándolos, o neutralizando o mermando la autonomía, la toma de decisiones o las opciones de los usuarios, tampoco a través de una interfaz digital de usuario o de una parte de ella"[82].

7. DIRECTIVA DE SERVICIOS FINANCIEROS A DISTANCIA DE 2023

La Directiva (UE) 2023/2673 de 22 de noviembre de 2023 por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia[83] explicita que las *"Dark patterns"*, es decir, los elementos engañosos "en las interfaces en línea de los comerciantes son

80. Art. 4.4 RD.
81. Cfr. arts. 5 y 7 RD.
82. Art. 6.2.a) RD.
83. Sobre la DSFD en la reciente doctrina *vid.*, GONZÁLEZ JIMÉNEZ, P. M., *La contratación a distancia de servicios financieros con consumidores tras la Directiva (UE) 2023/2673*, Aranzadi La Ley, 2025, pp. 217 y ss., en la que el citado autor analiza con profusión de detalla y acierto la configuración del derecho de desistimiento y protección contra patrones oscuros en interfaces en línea en esta sede.

prácticas que distorsionan o merman sustancialmente, bien de forma deliberada, bien de forma efectiva, la capacidad de los consumidores destinatarios del servicio financiero de tomar decisiones autónomas e informadas", lo que ocurre en los contratos de servicios financieros celebrados a distancia.[84]. La Directiva de Servicios Financieros a Distancia de 2023 establece una regulación complementaria al Reglamento de Servicios Digitales y obliga a los Estados miembros a impedir que los comerciantes que ofrezcan servicios financieros a distancia utilicen dichos elementos al celebrar contratos para dichos servicios. En este sentido, prevé que los servicios financieros puedan necesitar requisitos más detallados y posibilita que los Estados miembros introduzcan disposiciones más estrictas

8. REGLAMENTO DE INTELIGENCIA ARTIFICIAL DE 2024

Por su parte, el Reglamento de Inteligencia Artificial de 2024 no cita expresamente a las *"Dark Patterns"* como tal, pero sí conductas con las que se identifican, como es de ver en el Cdo. 29 al describir como "(l)as técnicas de manipulación que posibilita la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas (…)". En este sentido, y como reacción a dicha posibilidad se prevé en el artículo 5 del Reglamento de Inteligencia Artificial la prohibición de un conjunto de prácticas de inteligencia artificial, entre las que se encuentra "la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de forma apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas"[85].

9. NECESIDAD DE MAYOR COHESIÓN DE LA NORMATIVA REGULADORA DE LAS "DARK PATTERNS"

A la vista de los anteriores instrumentos normativos se puede concluir que en los últimos años se está intentando cohesionar la regulación de las *"Dark Patterns"*, así los más recientes Reglamentos sobre materias que se

84. Cdo. 41 DSFD.
85. Art. 5.1.a) RIA.

desarrollan en el ámbito digital preservan la aplicación preferente de la Directiva de Prácticas Comerciales Desleales con Consumidores y del Reglamento General de Protección de Datos. Esta articulación mínima resulta coherente y debe ser bienvenida, pero por otra parte no merma la necesidad de cohesionar la protección brindada por las diferentes normas de Unión Europea que regulan las interfaces engañosas en aras de aclarar el ámbito de aplicación de cada una, la esfera nacional o europea en la que están llamada a desplegar sus efectos, así como el objeto y alcance de cada normativa, el carácter de los daños[86], las consecuencias jurídicas aparejadas y acciones legales previstas y otros aspectos de índole procesal como la legitimación activa y pasiva, de gran relevancia a la hora de combatir este nuevo tipo de prácticas engañosas.

IV. REGULACIÓN FUTURA SOBRE "EQUIDAD DIGITAL"

El pasado 4 de octubre de 2024 se publicó el *"Digital Fairness Fitness Check"*[87]. Esta iniciativa forma parte de la agenda *"Better Regulation"* de la Unión Europea[88] y se proyecta sobre tres directivas relacionadas con la protección de los consumidores[89]. En particular, el *"Digital Fairness Fitness Check"* analizó la Directiva sobre Prácticas Comerciales Desleales, la Directiva 2011/83/EU sobre Derechos de los Consumidores y la Directiva 93/13/EEC sobre Cláusulas Contractuales Desleales. En la *"Digital Fairness Fitness Check"* la Comisión Europea recurre al concepto de "equidad digital" para referirse al alto nivel de protección de los consumidores, de conformidad

86. *Vid.*, SANTOS, S.; MOROZOVAITE, V. & DE CONCA, S., "No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws", *Information & Communications Technology Law*, 2025, pp. 1-47, en concreto, en las conclusiones (p. 42), al explicar sobre los daños: "We noted divergences, both in theanalysed literature review and policy studies, as harms are defined and described with ter-minological inconsistencies, ultimately hampering the application of national levelredress mechanisms. While policymakers and scholarly literature confirm that dark patterns cause harm both at individual and collective level, the effective redress of theharm caused by dark patterns faces several challenges for both material, non-materialand collective harms".

87. *Vid.* EUROPEAN COMISSION, *Comission Staff Working Document Fitness Check of EU consumer la won digital fairness*¸ Brussels, 3.10.2024 SWD(2024) 230 final, pp. 1-218 (en adelante *"Digital Fairness Fitness Check"* o DFFC). *Vid.* también el portal web de la Comisión Europea, sobre la publicación del *"Study to support the fitness check of EU consumer law on digital fairness and report on the application of the Modernisation Directive"*.

88. *Vid.* DFFC, p. 8.

89. En concreto, la DPCD, así como la Directiva 2011/83/EU sobre derechos de los consumidores y la Directiva 93/13/EEC de condiciones contractuales desleales.

con el artículo 169 del Tratado de Funcionamiento de la Unión Europea, que también debe garantizarse en el entorno digital[90].

El *"Digital Fairness Fitness Check"* mostró los resultados del control de adecuación de las citadas normativas sobre consumidores y sus objetivos, para identificar solapes, incoherencias y sinergias[91]. En este sentido abarcó cinco dimensiones entendidas como criterios clave de evaluación como son la eficacia, eficiencia, relevancia, coherencia y valor añadido en la Unión Europea[92], todo ello con miras a identificar necesidades actuales y también la adecuación de dichas normativas en atención a los avances normativos y tecnológicos en el ámbito de la digitalización, en el que las *"Dark Patterns"* constituyen un claro ejemplo de prácticas problemáticas en este ámbito. Además de ofrecer una definición sobre *"Dark Patterns"* (o diseños engañosos)[93], se indica, en relación con el marco regulatorio, que Directivas analizadas abordaban las interfaces engañosas parcialmente y que solo un número limitado de *"Dark Patterns"* están prohibidos directamente en la lista negra de la Directiva de Prácticas Comerciales Desleales con Consumidores, ninguna de las prohibiciones se refiere de forma específica a las interfaces digitales y, además, su aplicación depende de una evaluación "caso por caso"[94].

A estos efectos, el *"Digital Fairness Fitness Check"* informa con claridad que la falta de certeza jurídica sobre la imparcialidad o injusticia de tipos específicos de *"Dark Patterns"* en la Directiva de Prácticas Comerciales Desleales con Consumidores podría socavar la eficacia de su aplicación[95]. Por otra parte, se informa que el Reglamento de Servicios Digitales contiene regulación que aborda algunos aspectos de las interfaces engañosas, si bien aprecia que su alcance difiere en atención al "acervo horizontal en materia de consumo"[96]. Asimismo, desde la perspectiva de algunos *"stakeholders"*

90. *Ibid.*, p. 1.
91. *Vid.* DFFC, p. 8.
92. *Ibid.*, p. 2.
93. *Ibid.*, p. 145: "The term dark patterns (or deceptive design) refers to commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise, e.g. presenting choices in a non-neutral manner, using fake countdown timers to create urgency, using emotional manipulation to make consumers second-guess their indicated choice, phrasing questions using double negatives, misleading consent options, e.g. in cookie banners".
94. *Vid. ult. loc.* (traducción libre).
95. *Ibid.*, p. 148: "However, the lack of legal certainty about the fairness or unfairness of specific types of dark patterns under the UCPD could undermine the effectiveness of its application".
96. *Ibid.*, p. 151 (traducción libre).

y autoridades, las acciones legales para el cumplimiento pueden ser más eficaces si los tribunales y las autoridades pueden señalar prácticas específicas en la lista negra de la Directiva de Prácticas Comerciales Desleales[97]. Por otra parte, también se afirma que la prohibición de prácticas agresivas (inicialmente pensada para escenarios *offline*), podría ser considerada desde una nueva perspectiva en "la era digital"[98].

El *"Digital Fairness Fitness Check"* concluye al respecto que, en primer lugar, la normativa en materia de consumo de la Unión Europea analizada no parece ser lo suficientemente clara ni eficaz para abordar los *"Dark Patterns"*; en segundo lugar, que esta circunstancia socava la aplicación efectiva de varios derechos de los consumidores, y, en tercer lugar, que esta situación "cuestiona la capacidad del consumidor medio o el consumidor vulnerable para tomar decisiones informadas sobre sus transacciones en el entorno digital"[99]. Finalmente, *"Digital Fairness Fitness Check"* ofrece una serie de conclusiones generales, entre la que se encuentra la referente a que los patrones oscuros no se pueden resolver de manera adecuada solo proporcionando más información a los consumidores. Otra conclusión de interés se refiere al hecho de que los comerciantes respetuosos con la ley no tienen la certeza suficiente de que las medidas que adoptan sean suficientes para garantizar el cumplimiento, al tiempo que carecen de incentivos para esforzarse en un entorno competitivo "que no premia la equidad digital desde el diseño". En este sentido se concluye que, pese a que las directrices interpretativas de la Comisión se valoran de forma positiva, "no son vinculantes y no pueden crear incentivos suficientes para garantizar una aplicación efectiva". Por otra parte, se explica que las iniciativas voluntarias, como los códigos de conducta pueden mejorar la aplicación de la legislación "pero en última instancia no pueden subsanar las deficiencias del marco legislativo"[100].

Este escenario ha auspiciado la propuesta de la denominada futura *"Digital Fairness Act"*[101]. Sin embargo, a la fecha es escasa la información al respecto. En este sentido, voces en la doctrina internacional[102] han puesto

97. *Ibid.*, p. 149 (traducción libre).
98. *Vid. ult. loc.*, (traducción libre), si bien como informa el DFFC a la fecha solo una de las tres sentencias del TJUE se refiere a un escenario digital, escasez que se repite en escenario de la jurisprudencia nacional de cada Estado miembro.
99. *Ibid.*, p. 153 (traducción libre).
100. *Ibid.*, p. 88 (traducción libre).
101. *Ibid.*, p. 144.
102. *Vid.* NIKIFOROV, L., *Digital Fairness Act: If and How*, Brussels Privacy Hub, (post October 30, 2024) (disponible en: http://dx.doi.org/10.2139/ssrn.5025754) (última consulta: 7.7.2025), p. 2.

de manifiesto diversas críticas, como son la correspondiente a la vaguedad del concepto *"Digital Fairness"*, lo que dificulta su aplicación uniforme en los mercados digitales[103]. Además, se han indicado algunas dudas sobre la idoneidad de una nueva normativa en este sentido a la luz de los riesgos que puede entrañar, como son los derivados de un "exceso de regulación" que podría conllevar el "ahogo de la innovación"[104], así como el solapamiento e incremento de la complejidad en relación con otras normativas europeas existentes[105], las posible dudas sobre el conocimiento de los consumidores y cumplimiento de sus derechos, dada la realidad de los diferentes Estados miembro[106], o por el denominado "paternalismo" con respecto al consumidor[107], así como, finalmente, en atención a la concisión de la terminología empleada. Por todo ello, se ha concluido que, si bien es cierto que la Directiva de Equidad Digital o *"Digital Fairness Act"* puede mejorar la protección de los consumidores, también lo que existen dudas sobre su idoneidad[108].

V. A MODO DE CONCLUSIÓN

En la actualidad no cabe duda de la importancia económica y jurídica que han adquirido las interfaces engañosas, denominadas *"Dark Patterns"*, lo que se refleja en los múltiples instrumentos normativos de la Unión Europea llamados a ofrecer protección frente a este fenómeno. Existen hitos recientes en la regulación de los patrones oscuros como es de ver en el artículo 25 del Reglamento de Servicios Digitales que regula, por primera vez de forma expresa, la prohibición de los patrones oscuros en este ámbito, al tiempo que ha generado dudas con respecto a su articulación con la Directiva de Prácticas Comerciales Desleales con Consumidores y el Reglamento General de Datos.

---

103. *Ibid.*, p. 5.
104. *Ibid.*, pp. 5 y 6, al afirmar, por una parte, que "A Digital Fairness Act may potentially harmonize an existing gap in member states legislation and uniformise the Union's approach. In consequence, it may reduce uncertainty and hypothetically boost a cross-border commercial enterprises and transactions". Sin embargo, por otra: "This may lead to negative externalities in European competition and market such as an additional regulatory pressure and enhanced lobbying from larger companies, while stifling with compulsory, complicated and diverse measures small and medium enterprises in the EU".
105. *Ibid.*, p. 6.
106. *Vid. ult. loc.*
107. *Ibid.*, p. 7, al afirmar: "Another potential critique could come from those who believe that the Digital Fairness Act may be overly paternalistic, restricting consumer autonomy (…)".
108. *Ibid.*, p. 8.

Además, en los últimos años han aparecido diversos instrumentos normativos en la Unión Europea, que al abordar la regulación de materias relacionada con facetas digitales brindan nueva regulación a las interfaces engañosas, pero orientada a un ámbito de aplicación y a unas consecuencias jurídicas específicas. Todo ello exige, además, analizar caso a caso cada supuesto de interfaz engañosa, lo que resta operatividad al sistema de protección del consumidor, y, en definitiva, a la construcción de un mercado único digital más robusto. En sentido, diferentes sectores en la doctrina internacional han puesto de manifiesto la necesidad de mayor certeza, lo que no necesariamente debe derivar de más regulación. Tal vez fuera oportuna la publicación de directrices interpretativas que aclaren los anteriores aspectos.

Sin embargo, recientemente, el *"Digital Fairness Fitness Check"* de octubre de 2024 concluyó, en lo que ahora interesa, que los patrones oscuros no se pueden resolver solo mediante más información a los consumidores, y que, aunque las directrices interpretativas de la Comisión se valoran de forma positiva, "no son vinculantes y no pueden crear incentivos suficientes para garantizar una aplicación efectiva". En este contexto cobra interés el desarrollo de una futura normativa sobre "equidad digital" a través de una nueva *"Digital Fairness Act"*. No obstante, a la fecha, a las ventajas de pueda acarrear también se han opuesto diversas críticas.

En cualquier caso, tal vez la *"Digital Fairness Act"* pueda ser el instrumento normativo de la Unión Europea que sirva de ocasión para abordar de una forma unitaria la protección frente a las *"Dark Patterns"* y su definición, al tiempo que la regulación de los incentivos en el diseño de interfaces que compitan de manera leal, y, finalmente, los cauces por los que articular la regulación (fragmentaria) existente y aportar mayor claridad y certeza jurídica sobre las remedios jurídicos en la Unión Europea frente a las *"Dark Patterns"* y otros fenómenos propios de la incesante digitalización.

BIBLIOGRAFÍA

BELL, D., *The Coming of Post-Industrial Society. A Venture in Social Forecasting*, Basic Books, New York, 1973, pp. 1-507.

BRENNCKE, M., "Regulating dark patterns", *Notre dame J. Int'L & Comp. L.* Vol. XIV: I, p. 16.

BRIGNULL, H., LEISER, M., SANTOS, C., & DOSHI, K. (2023, April 25). *Deceptive patterns — user interfaces designed to trick you*. deceptive.design. Retrieved April 25, 2023, from https://www.deceptive.design/ (fecha de consulta: 10.12.2023).

CASADO, A., *Prácticas desleales en entornos digitales*, Tirant Lo Blanch, Valencia, 2025, pp. 1-417.

CASTELLÓ PASTOR, J. J. (Dir.), *Análisis del reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 1-474.

CAUFFMAN, C., KAMPERMAN SANDERS, A., and TYAGI, K. (eds.), *Digital Platforms, Competition Law, and Regulation: Comparative Perspectives*, Hart Publishing, London, 2024, pp. 1-246.

DAY, G., and STEMLER, S., "Are dark patterns anticompetitive", *Alabama Law Review*, Vol. 72:1:1, 2020, pp. 1-45.

DRUCKER P. F., *The age of discontinuity. Guidelines to Our Changing Society*, William Heinemann, London, 1969, pp. 1-368.

GONZÁLEZ JIMÉNEZ, P. M., *La contratación a distancia de servicios financieros con consumidores tras la Directiva (UE) 2023/2673*, Aranzadi La Ley, 2025, pp. 1-287.

GRAEF, I., "The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?" (April 3, 2023). Forthcoming as a book chapter in WOODCOCK, R. A., *Toward an Inframarginal Revolution: Markets as Wealth Distributors*, Cambridge University Press 2023, TILEC Discussion Paper No. 2023-07, Tilburg Law School Research Paper, pp. 1-21.

HAYEK F. A., The Use of Knowledge in Society, *American Economic Review,* XXXV, N.º 4, 1945, pp. 519-530.

HERMAN J., Dark patterns: EU's regulatory efforts. *Security and Privacy*. 2024; 7(6):e441. (doi: 10.1002/spy2.441).

KAPROU, E., "Aggressive commercial practices 2.0: Is the UCPD fit for the digital age?", *Journal of European Consumer and Market Law*, no. 2, 2023, pp. 76-84.

LEISER, M. and SANTOS, C., *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface* (April 27, 2023), pp. 1-31 (Available at SSRN: https://ssrn.com/abstract=4431048) (última consulta: 5.7.2025).

LEISER, M., *Illuminating Manipulative Design: from "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair*

Commercial Practices Directive (April 14, 2022), pp. 1-31. Available at SSRN: https://ssrn.com/abstract=4418586 (última consulta: 5.7.2025).

MACHLUP, F., *The production and distribution of knowledge in the United States*, Princeton University Press, Princeton, NY, 1962, pp. 1-416.

MASUDA, Y., *The Information Society as Post Industrial Society*, Institute for the Information Society, Tokyo, Japan, 1980, pp. 1-158, y World Future Society, Washington, D.C., USA, 1981, pp. 1-178.

MATO PACÍN, M.ª, N., *Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros*, Agencia Estatal BOE, Colección Derecho Privado 29, Madrid, 2024, pp. 1-146.

NIKIFOROV, L., *Digital Fairness Act: If and How*, Brussels Privacy Hub (post October 30, 2024), pp. 1-8. (disponible en: http://dx.doi.org/10.2139/ssrn.5025754) (última consulta: 7.7.2025).

OECD, "Dark commercial pattern", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, 2022, pp. 1-96.

SADIN, E., *La humanidad aumentada*, Caja Negra, Ciudad Autónoma de Buenos Aires (Argentina), 2017, pp. 1-160.

SANTOS, S.; MOROZOVAITE, V. & DE CONCA, S., "No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws", *Information & Communications Technology Law*, 2025, pp. 1-47.

Capítulo 4

Dudas sobre el funcionamiento de los órganos de solución extrajudicial certificados en el marco del Reglamento de Servicios Digitales*

Rosa Pla Almendros
FPU Derecho Internacional Privado
Universitat de València

SUMARIO: I. PLANTEAMIENTO INICIAL. II. A MODO DE CONTEXTO: ASPECTOS REGULADOS Y NO REGULADOS POR EL ART. 21 RSD. III. ÓRGANOS CERTIFICADOS. IV. CONCRECIÓN DE ALGUNOS EXTREMOS POR LOS ÓRGANOS CERTIFICADOS. 1. *Ámbito de actuación*. 1.1. ADROIT. 1.2. User Rights. 1.3. Tanács. 1.4. Appeals Centre. 1.5. RTR. 1.6. ADR Center. 2. *Lengua del procedimiento*. 3. *Plazo para interponer la reclamación*. 4. *Tercero encargado de resolver la disputa*. 5. *Costas y honorarios*. V. PROBLEMAS DETECTADOS Y SOLUCIONES PROPUESTAS. BIBLIOGRAFÍA.

I. PLANTEAMIENTO INICIAL

El Reglamento de Servicios Digitales[1] (en adelante, "RSD") no es la primera norma europea que crea nuevos medios de solución extrajudicial destinados a proteger a los usuarios digitales frente a los riesgos (transfron-

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de trabajo es miembro la autora. Estudio realizado durante la estancia de investigación en el Max Planck Institute for Comparative and International Private Law de Hamburgo (Alemania).

1. Reglamento (UE) 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). *DO núm. L 277 de 27 de octubre de 2022*.

terizos) de internet. A este respecto, se pueden citar la Directiva 2013/11/UE[2] (actualmente en proceso de reforma[3]), el art. 28.ter.7 de la Directiva 2018/1808 de servicios de comunicación audiovisual[4], los arts. 17.9 y 21 de la Directiva 2019/790 de derechos de autor[5], el art. 10 del Reglamento 2021/784 de lucha contra la difusión en línea del contenido terrorista[6] y los arts. 11 y 12 del Reglamento 2019/1150 *Platform-to-Business*[7], sirviendo estos últimos de inspiración directa para los mecanismos incorporados por el RSD[8].

Sin perjuicio de lo anterior, la inclusión de los medios de solución extrajudicial en los arts. 20 y 21 del Reglamento de Servicios Digitales fue noto-

2. Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n o 2006/2004 y la Directiva 2009/22/CE (Directiva sobre resolución alternativa de litigios en materia de consumo). *DO núm. L 165 de 18 de junio de 2013*.
3. Resolución del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva 2013/11/UE, relativa a la resolución alternativa de litigios en materia de consumo, así como las Directivas (UE) 2015/2302, (UE) 2019/2161 y (UE) 2020/1828 (COM (2023)0649-C9-0384/2023-2023/0376(COD)), recientemente modificada por el propio Parlamento Europeo a través de la Modificación de la Directiva relativa a la resolución alternativa de litigios en materia de consumo, de 27 de febrero de 2025, (C/2025/1028). Para ver el estado del proceso de reforma, consúltese el siguiente enlace: https://www.europarl.europa.eu/legislative-train/theme-supporting-people-strengthening-our-societies-and-our-social-model/file-revision-of-the-alternative-dispute-resolution-framework, último acceso el 9 de mayo de 2025.
4. Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), *DO núm. L 3030, de 28 de noviembre de 2018*.
5. Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/ CE, *DO núm. L 130, de 17 de mayo de 2019*.
6. Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea, *DO núm. L 172, de 17 de mayo de 2021*.
7. Reglamento (UE) 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, *DO núm. L 186, de 11 de julio de 2019*.
8. Para un análisis más profundo del solapamiento y posible coordinación entre los citados medios de solución extrajudicial con los incorporados por el RSD, véase PLA ALMENDROS, R., *La solución extrajudicial de disputas transfronterizas en el Reglamento de Servicios Digitales*, Colex, A Coruña, 2025, pp. 186-209.

riamente aplaudida por la doctrina, toda vez que por primera vez se permitiría a los usuarios digitales impugnar las decisiones de moderación de contenidos diariamente adoptadas por las plataformas en línea a través de una tutela distinta a la judicial. En particular, exponentes de la academia tanto internacional como nacional se pronunciaron a su favor.

Sin ánimo de exhaustividad, HUSOVEC concibió esta "segunda opinión experta" como un remedio rápido y barato potencialmente capaz de reducir los fallos en la moderación de contenidos de las plataformas[9] y ORTOLANI afirmó que se trataban de disposiciones necesarias para garantizar el acceso a la justicia[10]. En el ámbito nacional, LLOPIS NADAL, entre otros, los consideró esenciales para ofrecer a los usuarios digitales vías de tutela distintas a la judicial, la cual, como es sabido, queda descartada la mayoría de las veces[11], y CASTELLÓ PASTOR abaló que aumentaran "la seguridad jurídica y las garantías procesales de los comerciantes y los destinatarios del servicio, además de fortalecer la confiabilidad del entorno digital"[12].

La bienvenida que dieron los académicos a estos preceptos se manifestó sobre todo unos meses antes de la entrada en funcionamiento del RSD (febrero de 2024). Se trataba de un momento en el que los medios extrajudiciales del art. 21 RSD todavía estaban pendientes de implementación, de modo que no existían aún órganos que se hubieran certificado para resolver disputas en virtud del mencionado artículo. Así las cosas, la vaguedad y la amplitud de la redacción del art. 21 RSD, que como se verá no concreta demasiados extremos acerca del funcionamiento de los mencionados órganos, provocaron que aquellas opiniones doctrinales tan solo pudieran limitarse

9. HUSOVEC, M., "Will the DSA work?: On Money and Effort", en HOBOKEN, J., et al. (eds.), *Putting the DSA into Practice,* Verfassungsbooks, 2023, pp. 19-35, p. 26. Versión en línea accesible en: https://ssrn.com/abstract=4384266, último acceso el 9 de mayo de 2025.
10. ORTOLANI, P., "The resolution of content moderation disputes under the Digital Services Act", *Giustizia Consensuale*, núm. 2 (2022), pp. 1-21, p. 2.
11. LLOPIS NADAL, P., "Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales", en HERNÁNDEZ SAINZ, E., MATE SATUÉ, L. C., y ALONSO PÉREZ, M.T. (coords.), *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales*, Colex, A Coruña, 2023, pp. 140-173, p. 148.
12. CASTELLÓ PASTOR, J. J., "Interrelación del reglamento de servicios digitales con el reglamento *platform to business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en CASTELLÓ PASTOR, J. J., (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, Navarra, 2024, pp. 361-398, p. 385.

a divagar y especular sobre el mejor o peor funcionamiento que pensaban que caracterizaría a los órganos en cuestión una vez se pusieran en marcha.

En el momento de escribir estas líneas, tras un año de aplicación del Reglamento de Servicios Digitales, ya se han acreditado —o, en la terminología propia del RSD, "certificado"— seis órganos de solución extrajudicial al amparo del art. 21 RSD[13]. En consecuencia, esta realidad ofrece la posibilidad de analizar la manera en que estos órganos han concretado algunas de las cuestiones procedimentales que hasta ahora no se podían descifrar por no quedar reguladas en el art. 21 RSD. A través de un análisis de estos aspectos, el objetivo del estudio, que adoptará principalmente la perspectiva de los usuarios digitales, será concluir si los órganos acreditados con arreglo al precepto en cuestión constituyen, tal y como pretenden, una vía eficaz de protección de las víctimas de las decisiones de moderación de contenidos.

Sentado lo anterior, el capítulo tomará como punto de partida un breve repaso del funcionamiento del art. 21 RSD. Tras ello, se listarán los órganos que se han certificado con arreglo a dicho precepto a fecha de 9 de mayo de 2025, que se corresponde con la última fecha de actualización de la investigación. Más tarde, se estudiará la manera en que estos órganos han concretado algunos de los extremos del procedimiento a los que el art. 21 RSD no prestaba atención. Por último, tan solo restará concluir, presentando los problemas detectados y tratando de ofrecer soluciones a los mismos.

II. A MODO DE CONTEXTO: ASPECTOS REGULADOS Y NO REGULADOS POR EL ART. 21 RSD

Como es sabido, uno de los rasgos característicos y comunes a las denominadas "leyes digitales europeas" es la consecución de un doble objetivo. En este sentido, a la meta tradicional de contribuir al correcto funcionamiento del mercado interior, se les ha unido la necesidad de proteger los derechos fundamentales, en consonancia con el conocido como "constitucionalismo digital europeo"[14].

Como ejemplo paradigmático de las mencionadas leyes digitales europeas, el Reglamento de Servicios Digitales ha incorporado como meta en

13. https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement, último acceso el 9 de mayo de 2025.
14. Para más detalle, véase la obra paradigmática al respecto: DE GREGORIO, G., *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022.

su art. 1.1 RSD la consecución de un entorno en línea seguro y fiable y de la protección efectiva de los derechos de la Carta de Derechos Fundamentales de la UE ("CDFUE"[15]). Una de las principales manifestaciones de esta ambición declarada es la tutela de los usuarios digitales frente a las decisiones (automatizadas) de moderación de contenidos adoptadas por las plataformas en línea, que suelen errar por exceso[16], vulnerando derechos como la libertad de expresión o información[17], consagrados en el art. 11 CDFUE y claves para el mantenimiento de la democracia[18].

Las decisiones de moderación de contenidos[19], en sentido estricto, pueden ser potencialmente adoptadas por cualquier prestador de servicios intermediario, si bien aquí las restringiremos a las emitidas por los prestadores de plataformas en línea, por ser los únicos sujetos obligados por los arts. 20 y 21 RSD. Si se recuerda, estas decisiones pueden guardar un doble sentido.

a) Por un lado, si la plataforma en línea considera que un usuario digital ha proporcionado contenidos ilícitos o incompatibles con sus condiciones generales (ya sean fotografías, vídeos, comentarios, etc.)[20], adoptará una decisión atacando el contenido en cuestión o

15. Carta de los Derechos Fundamentales de la Unión Europea. *DO núm. C 202 de 7 de junio de 2016.*
16. Para más detalle sobre la moderación de contenidos de las plataformas en línea de muy gran tamaño tras la entrada en funcionamiento del Reglamento de Servicios Digitales, véase CASTELLÓ PASTOR, J.J, "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, vol. 17, núm. 1 (2025), pp. 308-328.
17. QUINTAIS, J. P., APPELMAN, N. y FATHAIGH, R., "Using Terms and Conditions to apply Fundamental Rights to Content Moderation", *German Law Journal,* núm. 24 (2023), pp. 881-911, p. 882, y FROSIO, G., y GEIGER, C., "Taking fundamental rights seriously in the Digital Services Act's Platform liability regime", *European Law Journal*, vol. 29, núm. 1-2 (2023), pp. 31-77, pp. 45 y ss.
18. LOI, M., "Making sense of the Digital Services Act. How to define platforms' systemic risks to democracy", *AW AlgorithmWatch gGmbH* (2023), pp. 1-21, p. 5.
19. Recuérdese que el art. 3.t) RSD define la moderación de contenidos como aquellas "*actividades, estén o no automatizadas, realizadas por los proveedores de servicios intermediarios, que estén destinadas, en particular, a detectar, identificar y actuar contra contenidos ilícitos o información incompatible con sus condiciones generales* (…)".
20. El RSD define las condiciones generales en el art. 3.u) y el contenido ilícito en el art. 3.h), si bien con respecto a este último ya ha sido de sobra argumentado que el precepto en cuestión no ofrece una verdadera definición, limitándose a confirmar que es contenido ilícito aquel que sea contrario al derecho de la UE o nacional de los Estados miembros. A fin de remediar este silencio, el coordinador de servicios digitales austriaco, en colaboración con la Comisión Europea, elaboró el pasado 25 de marzo de 2024 una suerte de guía sobre los contenidos que deben tildarse de ilícitos.

al usuario digital que lo haya publicado. Esta decisión, que deberá ser comunicada sobre la base del art. 17 RSD, podrá manifestarse de diferentes maneras, explicitadas en los arts. 17.1 y 20.1 RSD, a saber: la retirada o bloqueo de la información controvertida, la restricción de su visibilidad, la suspensión o cesación total o parcial de la prestación del servicio al usuario digital, la suspensión o supresión de su cuenta, o la suspensión, cesación o restricción de la capacidad de monetizar la información.

b) Por otro lado, la plataforma también puede adoptar la decisión opuesta. Ello ocurrirá si un tercero, que normalmente será un notificante del art. 16 RSD o un alertador fiable del art. 22 RSD, señala un contenido por ser ilícito o contrario a los términos y condiciones de la plataforma, y esta considera que no lo es. En estos supuestos, la plataforma adoptará una decisión a favor del contenido controvertido. Esta decisión, que en esta ocasión debería ser comunicada al notificante con arreglo al art. 16.4 RSD, se emitirá con un sentido opuesto al anterior, optando por no retirar ni bloquear la información, no restringir su visibilidad, no suspender ni ceder la prestación del servicio al usuario digital, no suspender ni suprimir su cuenta, ni tampoco suspender, cesar ni restringir la capacidad de monetizar el contenido.

Para atacar cualesquiera de los dos tipos de decisiones anteriores, el Reglamento de Servicios Digitales ha puesto dos medios de solución extrajudicial (arts. 20 y 21 RSD) a disposición de los usuarios digitales afectados por aquellas, salvo cuando sean adoptadas por plataformas en línea que sean pequeñas empresas o microempresas (art. 19 RSD). En síntesis, el art. 20 RSD obliga a las plataformas en línea a incorporar un sistema interno de solución extrajudicial que permita a los usuarios digitales afectados pre-

---

Esta lista, cuya meta es armonizar la aplicación del RSD, tiene un carácter meramente indicativo e incluye contenidos relacionados con el bienestar animal (venta ilegal), el incumplimiento de obligaciones de información (productos engañosos), violaciones de protecciones de datos e intimidad, declaraciones ilegales (calumnias, discriminaciones, odio), infracciones de derechos de propiedad industrial e intelectual, la manipulación electoral, comportamientos indeseables (*deepfakes*), acoso o intimidación en línea, pornografía (abuso sexual), también infantil, peligros para la seguridad y salud pública, fraudes o engaños, incitación al suicidio, contrabando con productos ilegales, violencia de género, explotación humana o trata de seres humanos. Para mayor detalle, véase la referida guía KOMMAUSTRIA, "Artículo 21 RSD. Órganos extrajudiciales de resolución de litigios. Información para los solicitantes", 25 de marzo de 2024, pp. 1-16, pp. 14-16, accesible en: https://www.rtr.at/medien/was_wir_tun/DigitaleDienste/Regelungen/Streitbeilegungsstellen.de.html, último acceso el 9 de mayo de 2025.

sentar reclamaciones frente a las decisiones de moderación de contenidos adoptadas por la plataforma. Por su parte, el art. 21 RSD, que lleva por rúbrica "Resolución extrajudicial de litigios", conduce a la creación de órganos extrajudiciales externos a las plataformas que se encargarán de resolver esas mismas disputas.

Conviene aclarar que la relación entre los mecanismos de los arts. 20 y 21 RSD es tanto alternativa como subsidiaria. Es decir, podría interponerse la reclamación haciendo uso del sistema interno de gestión de reclamaciones y, en caso de desacuerdo con el resultado, se podría acudir al órgano extrajudicial del art. 21 RSD. Pero también cabría acudir directamente a este último, sin que sea necesario pasar primero por el sistema interno del art. 20 RSD (art. 21.1 y cdo. 59 RSD)[21].

En nuestro caso, el foco se limitará al mecanismo creado por el art. 21 RSD, que constituye la verdadera novedad del RSD, toda vez que los sistemas internos de reclamaciones ya eran incorporados en muchas ocasiones de forma voluntaria por las plataformas en línea de muy gran tamaño[22]. Sentado lo anterior, el contenido del art. 21 RSD, aparentemente muy extenso, se puede reducir a dos aspectos.

Por un lado, el art. 21.3 RSD establece los requisitos que deben cumplir aquellos órganos que quieran ser certificados para atender las reclamaciones de solución extrajudicial. Una vez reúna estos requisitos, entre los que se incluyen la independencia y la imparcialidad, el órgano en cuestión deberá realizar una solicitud de certificación ante el coordinador de servicios digitales del Estado miembro donde vaya a establecerse. El coordinador comprobará que cumple con los requisitos y lo certificará, pudiendo desde entonces operar no solo en el Estado miembro de establecimiento, sino en toda la Unión Europea (cdo. 59 RSD).

Por otro lado, el resto del contenido del precepto en cuestión establece algunas directrices que deberán seguir los órganos acreditados al resolver las reclamaciones de que conozcan. Estas instrucciones son, sin embargo, reducidas, pudiéndose sintetizar en las cuatro siguientes.

---

21. Este carácter alternativo —además de subsidiario— entre los mecanismos de los arts. 20 y 21 RSD es aclarado de manera expresa por ADROIT, User Rights, Appeals Centre y ADR Center, si bien recomiendan agotar la vía del art. 20 RSD antes de acudir al art. 21 RSD.

22. WAGNER, G., Y EIDENMÜLLER, H., "Digital Dispute Resolution", *SSRN* (2021), pp. 1-44, pp. 17-18. Versión en línea accesible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871612, último acceso el 9 de mayo de 2025.

En primer lugar, se abordan los aspectos de legitimación activa y pasiva. Al respecto, se aclara que la primera le corresponde en exclusiva al usuario digital (art. 21.1)[23]. Este será quien interponga la reclamación y, además, quien decida ante cuál de todos los órganos de solución extrajudicial certificados quiere presentarla. Por su parte, la plataforma en línea siempre será la reclamada o legitimada pasiva, estando además por lo general obligada a colaborar en el procedimiento (art. 21.2 RSD).

En segundo lugar, se fija el plazo para resolver la reclamación en un plazo máximo de 90 días, prorrogable por otros 90 en caso de especial complejidad (art. 21.4 *in fine* RSD)[24].

En tercer lugar, la decisión por la que se resuelva la reclamación nunca será vinculante (art. 21.2 *in fine* RSD), pese a que algunos órganos hayan querido maquillar esta prohibición[25]. Asimismo, cabe destacar que, por una aplicación extensiva del art. 20.4 RSD, se puede entender que el contenido de la decisión tan solo podría limitarse a pronunciarse respecto a si la plataforma retiró o no el contenido de forma correcta, pero en ningún caso podría

23. Recuérdese que, a diferencia de lo que ocurre con el sistema interno de gestión de reclamaciones del art. 20 RSD, el legitimado activo solo podrá ser el usuario digital afectado por la decisión de forma directa o, en caso de haberlo, el notificante del art. 16 RSD, pero en ningún caso el usuario digital afectado de manera indirecta por la decisión. LLOPIS NADAL, P., "Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales", *op. cit*., p. 163.

24. La concreción de los supuestos en los que existe "especial complejidad" será una cuestión que deban dilucidar los órganos certificados. Mientras que la mayoría de ellos guarda silencio a este respecto, limitándose a reproducir en sus reglas de procedimiento esas mismas palabras, otros órganos han preferido concretarlas. A título de ejemplo, ADROIT define que la "especial complejidad" se produce cuando se manifiesten factores imprevisibles, como la complejidad de un asunto o un supuesto de fuerza mayor (ap. 7.a. de sus Reglas de procedimiento).

25. A título de ejemplo, el órgano húngaro Tanács establece de manera expresa que la decisión que emita podrá ser vinculante si la plataforma expresamente lo acepta (véase el apartado 3 de sus Reglas de procedimiento, que se remiten al art. 19.2.a) de la Act CIV of 2023 on certain rules regarding Internet intermediary services, al cual también se refiere el art. 13.2 del NMHH Decree No. 4/2024 (III.21) on the detailed rules regarding out-of-court dispute settlement bodies). En líneas similares se pronuncia el art. 10.1 de las Reglas de procedimiento del ADR Center. Estas afirmaciones, que en realidad se predican de todos los órganos certificados, aunque no lo digan expresamente, no deberían incluirse en las reglas de procedimiento de los órganos, pues pueden confundir al potencial legitimado activo, que podría llegar a pensar que las decisiones pueden ser vinculantes en ciertos casos.

otorgar otro tipo de tutela como la compensación por daños y perjuicios[26]. Para ello, habría de acudirse a la vía judicial del art. 54 RSD.

Por último, el art. 21.5 RSD también regula el régimen de costas y honorarios. En esencia, cada uno deberá satisfacer sus respectivos gastos derivados del proceso, salvo que el usuario digital viera su reclamación estimada y no hubiera actuado de mala fe, en cuyo caso la plataforma en línea reclamada debería satisfacer también las costas y los honorarios que en un principio quedaron a cargo del usuario. En relación con los honorarios, que deberán ser cuantificados por el órgano certificado, no podrán superar los costes en que incurra el órgano para resolver el procedimiento, y deberán ser muy reducidos o gratuitos para el usuario digital reclamante.

Además de todo lo anterior, nada más establece el art. 21 RSD con respecto al funcionamiento de los órganos extrajudiciales. Así las cosas, son los propios órganos de solución extrajudicial que se certifiquen los que deben concretar el resto de los extremos del procedimiento. Esta parquedad en las líneas procedimentales a seguir ha generado fuertes críticas entre la doctrina, dado que puede desembocar en una potencial fragmentación y, a la postre, en una eventual "carrera a la baja" (*race to the bottom*) de la calidad del procedimiento en la lucha por conseguir mayores reclamaciones[27].

Al margen de este posible escenario, queda claro que los órganos son los encargados de especificar extremos como la lengua del procedimiento, el plazo para interponer la reclamación, la complementariedad de los órganos con la vía judicial, el modelo de financiación o la necesidad de tener en cuenta los derechos fundamentales a la hora de emitir decisiones. Por cuestión de espacio, resultará inviable detenerse en analizar cada uno de estos extremos, muchos de los cuales, además, ya están siendo tratados por expertos en la materia[28].

---

26. HUSOVEC, M., "Certification of Out-of-Court Dispute Settlement Bodies under the Digital Services Act", *SSRN* (2023), pp. 1-12, p. 10. Versión en línea accesible en: https://ssrn.com/abstract=4501726, último acceso el 9 de mayo de 2025.
27. WIMMERS, J., "The out-of-court dispute settlement mechanism in the Digital Services Act. A disservice to its own goals", *Jipitec*, vol. 12, núm. 5 (2021), pp. 381-401, pp. 394-399.
28. Al respecto, resulta interesante conocer la labor de Article 21, una suerte de consejo asesor académico (*Academic Advisory Board*) puesto en marcha por el órgano certificado en Alemania, User Rights GbmH, que se reúne periódicamente para reflexionar y discutir los aspectos más problemáticos que puede suscitar la puesta en marcha de los órganos del art. 21 RSD. Las conclusiones de cada reunión quedan plasmadas en una especie de guía, que por el momento ha tratado el rol de los órganos del art. 21 RSD (agosto de 2024) y el papel de los derechos fundamentales en sus resoluciones (noviembre de 2024). Conviene destacar la rigurosidad científica y argumentativa de

En su lugar, la atención se restringirá a aquellas cuestiones que, aunque puedan parecer demasiado elementales o básicas, resultan sin duda esenciales para determinar si realmente los órganos del art. 21 RSD constituyen una vía de tutela eficaz para los usuarios digitales. En particular, estas cuestiones serán las cinco siguientes: el ámbito de actuación de los órganos, la lengua de solución de los procedimientos, el plazo para interponer la reclamación, el tercero que resuelve y el régimen de costas y honorarios.

Sentado lo anterior, primero se procederá a listar los órganos que han obtenido la certificación del art. 21 RSD, para más tarde estudiar cómo cada uno de ellos ha respondido a los cinco interrogantes antes planteados.

III. ÓRGANOS CERTIFICADOS

En la fecha en la que se redactan estas líneas, según la página web oficial que la Comisión Europea debe mantener por obligación del art. 21.8 RSD[29], los coordinadores de servicios digitales de los distintos Estados miembros (en adelante, "CSSDD"), en calidad de autoridades administrativas nacionales habilitadas para ello, han certificado un total de seis órganos de solución extrajudicial.

Por orden cronológico, estos han sido los siguientes. Primero, el CSSDD de Malta, Malta Communications Authority, fue pionero al certificar el primer órgano en julio de 2024, que lleva por nombre ADROIT[30]. Más tarde, el CSSDD alemán, Bundesnetzagentur, certificó el órgano de solución extrajudicial User Rights GmbH en agosto de 2024 (en adelante, "User Rights")[31]. Ese mismo mes, el CSSDD húngaro, Nemzeti Média-és Hírközlési Hatóság, acreditó a Online Platform Vitarendező Tanács (en adelante, "Tanács")[32]. En septiembre de ese mismo año, el CSSDD irlandés, Coimisiún na Meán, otorgó la certificación al órgano Appeals Centre Europe (en adelante, "Appeals Centre")[33]. El siguiente turno fue el del CSSDD austriaco, KommAustria, que certificó el órgano RTR-GmbH, Fachbereich Medien (en adelante, "RTR")[34]. Por último, el CSSDD italiano, AGCOM, en diciembre de 2024 autorizó al órgano ADR Center[35].

---

estos informes, emitidos por académicos del más alto nivel en la disciplina, como los Drs. João Pedro Quintais, Giovanni De Gregorio o Martin Husovec.

29. https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement, último acceso el 9 de mayo de 2025.
30. https://adroit.legal/, último acceso el 9 de mayo de 2025.
31. https://www.user-rights.org/en, último acceso el 9 de mayo de 2025.
32. https://opvt.hu/opvt, último acceso el 9 de mayo de 2025.
33. https://www.appealscentre.eu/, último acceso el 9 de mayo de 2025.
34. https://www.rtr.at/beschwerdeportal, último acceso el 9 de mayo de 2025.
35. https://adrcenter.it/, último acceso el 9 de mayo de 2025.

Tal y como permite el art. 21.6 RSD, la mayoría de los órganos certificados son de nueva creación, es decir, no existían con anterioridad a su certificación otorgada al amparo del RSD. Es el caso de ADROIT, User Rights, Tanács y Appeals Centre. Por el contrario, y también dentro del marco de posibilidades que brinda el art. 21.6 RSD, RTR es un órgano que ya existía para resolver las disputas extrajudiciales que surgieran en el marco de otras normas de la UE, entre las que se encuentra la Directiva 2018/1808 de servicios de comunicación audiovisual[36], y a las que ahora se suman las del art. 21 RSD. En la misma línea, el órgano ADR Center ya contaba con un largo recorrido previo, fundándose en 1998.

Con respecto a la forma de financiación de cada uno de los órganos, han optado por seguir distintos modelos. Recuérdese que el art. 21.3 RSD tan solo exige que los órganos sean financieramente independientes respecto de las plataformas en línea y de sus usuarios digitales, de modo que pueden emplear diversos modelos de financiación. Tal y como aclaró el coordinador de servicios digitales austriaco, estos incluyen la financiación pública y la financiación privada, ya sea íntegramente a través de las tasas cobradas por la resolución de litigios, ya sea mediante otras inyecciones de terceros[37].

Frente a este abanico de opciones, como se decía, los órganos no han adoptado una solución uniforme. User Rights, Tanács y Appeals Centre son de carácter privado —no se integran en ningún organismo público— y de sus ámbitos de aplicación se puede inferir que tan solo resuelven las disputas derivadas del art. 21 RSD. En consecuencia, lo más probable es que su financiación provenga de las tasas satisfechas por las plataformas en el marco de dichos procedimientos, tal y como afirma User Rights[38].

Por su parte, ADROIT también sigue un modelo de financiación privada, si bien en este caso se basa en las tasas cobradas por la resolución de litigios en virtud del art. 21 RSD, pero también del art. 12 del Reglamento

36. Así se desprende de las Directrices para la conciliación, resolución de disputas y procedimientos de quejas en RTR-GmbH, accesibles en https://www.rtr.at/medien/aktuelles/veroeffentlichungen/Veroeffentlichungen/Sonstiges/verfahrensrichtlinien_beschwerdestelle/Verfahrensrichtlinien.de.html, último acceso el 9 de mayo de 2025.

37. KOMMAUSTRIA, "Artículo 21 RSD. Órganos extrajudiciales de resolución de litigios. Información para los solicitantes", 25 de marzo de 2024, pp. 1-16, p. 5, accesible en: https://www.rtr.at/medien/was_wir_tun/DigitaleDienste/Regelungen/Streitbeilegungsstellen.de.html, último acceso el 9 de mayo de 2025.

38. En este caso, la página web del órgano aclara en su sección de preguntas frecuentes que "*We are independent and funded through fees paid by online platforms*".

P2B[39]. Respecto a ADR Center, este también disfruta de financiación privada: nació desde el principio como una SL —empresa privada—, aunque debe admitirse que en 2022 obtuvo la "*B-corp certification*" y adoptó legalmente la forma de "*Benefit company*", implicando que su objetivo ya no es solo el lucro económico, sino también el impacto positivo en la sociedad[40].

Por último, y a diferencia de todos los anteriores, el órgano RTR es de naturaleza pública y se integra dentro de RTR Medien, que es la Autoridad Reguladora austriaca para la radiodifusión y las telecomunicaciones, a la que pertenece KommAustria, una oficina administrativa designada como coordinador de servicios digitales en Austria.

El resto de los CSSDD de los Estados miembros todavía no ha certificado ningún órgano con arreglo al art. 21 RSD. Debe recordarse que el mencionado precepto no impone a los Estados miembros ni a sus CSSDD respectivos una obligación de acreditar órganos —son estos los que deben solicitar la certificación y no del revés—. De hecho, ni siquiera establece un número mínimo ni máximo de órganos que deban ser certificados.

En efecto, resulta llamativo que el CSSDD español, esto es, la Comisión Nacional de Mercados y de la Competencia (CNMC)[41], todavía no haya certificado ningún órgano. A este respecto, la situación es preocupante. En particular, pese a que la CNMC fue nombrada como CSSDD en España, dando cumplimiento a la obligación del art. 49 RSD —con un retraso de casi un año—[42], esta decisión no fue acompañada de una atribución de competencias. En consecuencia, la CNMC en la práctica se encontraba impedida para ejercer su rol como CSSDD y, por extensión, no podía certificar a ningún órgano que lo solicitara al amparo del art. 21 RSD.

El incumplimiento del Estado español ha irritado a la Comisión Europea, quien desde julio de 2024 lleva advirtiendo a España sobre la necesidad de otorgar competencias efectivas que permitan a la CNMC ejercer sus competencias como coordinador de servicios digitales conforme al RSD. Frente a

39. Pese a que es un órgano de nueva creación, ADROIT se ha concebido para resolver disputas en el marco del RSD, y también del Reglamento 2019/1150 *Platform-to-Business* antes citado (véase nota a pie 8), probablemente por motivos de financiación.
40. https://adrcenter.com/adr-center/our-past/, último acceso el 9 de mayo de 2025.
41. https://www.cnmc.es/prensa/coordinador-servicios-digitales-20240124, último acceso el 9 de mayo de 2025.
42. Los Estados miembros tenían hasta el 17 de febrero de 2024, fecha en que el RSD devenía de aplicación práctica, para nombrar a sus coordinadores de servicios digitales. Sin embargo, España no cumplió esta directriz hasta el 24 de enero de 2024, casi un año después.

fuentes que sugieren lo contrario[43], y pese a la insistencia de la UE, todavía no se ha dado cumplimiento a esta obligación, lo cual ha llevado a la Comisión Europea a iniciar el pasado 7 de mayo de 2025 un procedimiento de incumplimiento contra España ante el TJUE en virtud del art. 258 TFUE[44]. Bajo estas circunstancias, la CNMC todavía no se encuentra en condiciones de certificar órganos de solución extrajudicial cuando así se lo soliciten.

Pese a que se desconoce si existe algún organismo con la intención de pedir la certificación en España, recientemente se ha podido conocer que existen ya tres órganos candidatos que pretenden ser certificados en distintos Estados: Central European Appeals Hub (Eslovaquia), Impress Dispute Resolutions (Irlanda) y MFSD (Italia)[45].

En cualquier caso, pendientes de la futura certificación de los tres órganos antedichos, de momento no hay ningún órgano más autorizado aparte de los seis mencionados con carácter previo. Es cierto que la página web oficial de la Comisión Europea que tiene la obligación de comunicar este extremo no se actualiza desde el 12 de febrero de 2025, siendo posible que en el *interim* se haya certificado algún órgano que no aparezca todavía publicado. No obstante, sería algo extraño porque la Comisión tiene la obligación legal de mantener la lista "*actualizada*" (art. 21.8 RSD).

IV. CONCRECIÓN DE ALGUNOS EXTREMOS POR LOS ÓRGANOS CERTIFICADOS

Cada uno de los seis órganos certificados cuenta con una página web en la que publican unas reglas de procedimiento que concretan, entre otros extremos, los detalles del procedimiento no previstos por el art. 21 RSD[46]

43. https://comercioconectado.gob.es/es-es/EstaPasando/Paginas/gobierno-habilita-cnmc-coordinador-servicios-digitales-espa%C3%B1a.aspx, último acceso el 9 de mayo de 2025.
44. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081, último acceso el 9 de mayo de 2025.
45. Esta noticia fue publicada por el órgano ADROIT a través de su cuenta de LinkedIn durante la semana del 17 de abril de 2025, y es accesible a través del siguiente enlace: https://www.linkedin.com/company/adroit-legal/, último acceso el 29 de abril de 2025.
46. Las reglas de procedimiento de los órganos, pese a que deben ser de fácil acceso al público según el art. 21.3.f) RSD, no siempre lo son. En la mayoría de los casos, las reglas son accesibles desde la página web, siendo en algunos casos más sencillo encontrarlas que en otros. Ejemplos del primer caso son ADROIT (https://adroit.legal/rules_of_procedure/) y Appeals Centre (https://www.appealscentre.eu/rules-of-procedure/), y del segundo, RTR (https://www.rtr.at/medien/aktuelles/veroeffentlichungen/Veroeffentlichungen/Sonstiges/verfahrensrichtlinien_beschwerdestelle/Verfahrensri-

(en adelante, "Reglas" o "Reglas de procedimiento"). Como se dijo, a continuación, se abordarán cinco de estos aspectos, estudiando cómo los han resuelto cada uno de los órganos.

1. ÁMBITO DE ACTUACIÓN

Según el art. 21.1 RSD, el usuario digital legitimado podrá acudir a los órganos de solución extrajudicial certificados para interponer reclamaciones contra las decisiones de moderación de contenidos adoptadas por las plataformas en línea. De hecho, se permite que el usuario elija "*cualquier órgano de resolución extrajudicial de litigios que haya sido certificado*" para interponer su reclamación, con independencia de que este haya sido acreditado en uno u otro Estado miembro.

Sin embargo, dentro de aquella aparente amplitud, las Reglas de procedimiento de cada órgano condicionan las reclamaciones de las que podrá conocer cada uno de ellos. El resultado es que no todos los órganos certificados admitirán todas las reclamaciones interpuestas con arreglo al art. 21 RSD. Por supuesto, se trata de un extremo que deberá tener en cuenta el legitimado activo a la hora de decidir el órgano al que acude con su reclamación.

1.1. ADROIT

El órgano maltés ha sido certificado con un ámbito de actuación considerablemente amplio. En particular, podrá resolver disputas relacionadas con las decisiones que adopte cualquier plataforma en línea que se encuentre bajo el ámbito de aplicación del Reglamento de Servicios Digitales[47]. A este

chtlinien.de.html) y ADR Center (https://ods.adrcenter.it/en/regolamento.html). En el caso de User Rights, un escondite de la página web del órgano permite descargar las reglas en formato PDF (https://www.user-rights.org/en/how-it-works). Por último, el órgano húngaro Tanács es el que hace esta tarea más difícil. Además de que su página web tan solo esté disponible en húngaro, las reglas de procedimiento accesibles a través de su web son muy básicas y escuetas (https://opvt.hu/opvt/eljaras), y se remiten para mayor detalle a auténticas normas que regulan a los prestadores de servicios intermediarios en general (Act CIV of 2023 on certain rules regarding Internet intermediary services) o a los órganos de solución extrajudicial que puedan certificarse en Hungría en particular (NMHH Decree No. 4/2024 (III.21) on the detailed rules regarding out-of-court dispute settlement bodies). Último acceso a todos los enlaces el 9 de mayo de 2025.

47. El art. 3.i) RSD define una plataforma en línea como "*un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público*". En consecuencia, no debe adoptarse una óptica reduccionista que se limite a identificar las plataformas en línea con las redes sociales. Por el contrario, deben incluirse otras

respecto, debe recordarse que estas serán todas las plataformas en línea, que no sean microempresas ni pequeñas empresas (art. 19 RSD), y que ofrezcan sus servicios a usuarios digitales situados o establecidos en un Estado miembro de la UE, con independencia de que estén establecidas o no en la Unión, pero siempre que tengan una conexión sustancial con esta (arts. 2.1 y 3.d) y e) RSD).

En este caso, el órgano ADROIT concreta que, dentro de aquella categoría de plataforma en línea, tienen cabida plataformas muy diversas: plataformas de compras y reservas en línea, plataformas de intercambio de contenidos y marketing basado en contenidos, plataformas de crowdfunding y préstamos P2P, plataformas Web3, Defi, NFT y fintech, así como plataformas de juegos, apuestas y juegos de azar, y plataformas y mercados de comercio B2B, B2C y P2P.

El mencionado listado de plataformas no aparece en las Reglas de procedimiento de ADROIT, sino en su página web —que se refiere a ellas como "áreas de *expertise*"[48]—. Pese a ello, no debe restársele importancia, toda vez que el formulario de reclamación de ADROIT exige rellenar el tipo de plataforma frente a la que se reclama, y la respuesta a esta pregunta es cerrada, solo pudiéndose señalar alguno de los tipos de plataformas antes mencionados. Por tanto, parece que esta lista de plataformas debe entenderse con carácter exhaustivo, si bien la discusión sobre el carácter cerrado o abierto de esta lista no plantea problemas mayores, habida cuenta de que es tremendamente amplia y resulta difícil imaginar plataformas no incluidas en ella.

Desde el punto de vista objetivo, las reclamaciones podrán tener como base la ilicitud del contenido o su contrariedad con los términos y condiciones de la plataforma en cuestión. De nuevo, estos extremos no los concretan las Reglas, sino la página web del órgano, probablemente porque sea una cuestión ya aclarada por el art. 21 RSD —y no restringida por ADROIT—.

Y desde la perspectiva del legitimado activo, la reclamación podrá ser interpuesta por un usuario digital que resida en la UE, o por un usuario digital que resida fuera de esta, pero demuestre una "conexión razonable" con esta región (ap. 3.a Reglas ADROIT). Pese a que las Reglas de procedimiento no concreten esta conexión, en la sección de "Preguntas frecuentes" (*FAQ*) de la página web del órgano sí se pueden encontrar algunos ejemplos, como cuando el usuario digital publica un contenido desde fuera de la UE,

también comúnmente utilizadas, como los servicios de reserva de habitaciones de hotel, de vuelos, de restaurantes, de excursiones o eventos.

48. https://adroit.legal/, último acceso el 9 de mayo de 2025.

pero visualizado por usuarios que viven dentro de ella, o cuando se desarrollan aplicaciones fuera del mercado europeo para que operen en este. En cualquier caso, los ejemplos de extraterritorialidad —que deben valorarse positivamente[49]— no agotan todas las posibilidades de conexión sustancial con la UE, que deberán aclararse caso por caso.

1.2. User Rights

Este órgano certificado ya restringe su ámbito de actuación con respecto al anterior, si bien de nuevo lo hace en la página web y no en sus Reglas de procedimiento. En particular, solo resolverá los litigios relacionados con decisiones de moderación de contenidos emitidas por tres plataformas en línea de muy gran tamaño: Instagram, Tiktok o LinkedIn[50]. Por tanto, no se podrá acudir a este órgano para interponer reclamaciones contra cualquier otra plataforma. Conviene admitir, no obstante, que el órgano tiene la intención de ampliar las plataformas que pueden tener la condición de legitimada pasiva.

Con respecto al fundamento de la decisión, la web aclara que esta puede referirse a contenidos contrarios a los términos y condiciones de las mencionadas plataformas, o bien a los contenidos que sean ilícitos por ser contrarios al derecho de la UE o al derecho alemán. En consecuencia, las decisiones que retiren (o no) contenidos por ser contrarios a un derecho nacional distinto al alemán, no podrán ser impugnadas ante User Rights.

Por último, en este caso se guarda silencio sobre el lugar donde debe encontrarse o residir el usuario digital que interponga la reclamación. A inicios de abril de 2025, el formulario de reclamación de User Rights exigía que el usuario digital que interpusiera la reclamación afirmara que residía "permanentemente" en un Estado miembro como requisito de procedibilidad. Sin embargo, esta exigencia ha desaparecido a fecha de hoy.

1.3. Tanács

El órgano húngaro tan solo ha sido certificado para resolver las disputas que surjan con respecto a cualquier plataforma establecida en Hungría o cuyos servicios se dirijan a este país (art. 1.1 Act CIV of 2023 on certain rules regarding Internet intermediary services). De nuevo, las decisiones adop-

49. PALAO MORENO, G., "Avances en el sistema de resolución alternativa de litigios de consumo europeo adaptado a las controversias transfronterizas en el mercado digital", *Revista e-mercatoria*, vol. 23, núm. 2 (2024), pp. 67-104, p. 92.

50. https://www.user-rights.org/en, último acceso el 9 de mayo de 2025.

tadas por plataformas que operen en países de la UE, pero no en Hungría, no podrán ser impugnadas haciendo uso de este órgano.

En cuanto al fundamento de la decisión de moderación de contenidos que se ataca, se incluyen todos los del art. 21 RSD (art. 17.1 Act CIV of 2023 on certain rules regarding Internet intermediary services), de modo que puede estar fundada en la ilicitud del contenido o su contrariedad con los términos y condiciones de la plataforma en cuestión.

Para acabar, en este caso no se estipula de manera expresa dónde debe estar establecido el usuario digital para poder interponer una reclamación. Con base en una postura prudente, lo más razonable sería pensar que solo los establecidos en la UE podrían efectuar la reclamación de manera válida.

1.4. Appeals Centre

Este órgano vuelve a restringir el ámbito de reclamaciones de que potencialmente puede conocer. Así las cosas, deja claro que solo atenderá aquellas reclamaciones relacionadas con decisiones de moderación de contenidos que hayan sido adoptadas por Facebook, Tiktok o Youtube. De este modo, las quejas efectuadas en virtud del art. 21 RSD contra una plataforma distinta no podrán canalizarse a través de este órgano.

En el mismo sentido, las decisiones de las que puede conocer este órgano solo podrán basarse en la contrariedad del contenido con los términos y condiciones de la plataforma, pero se rechaza de manera expresa conocer del contenido ilícito[51], al menos de momento. Pese a que los términos y condiciones superan el ámbito material prohibido con arreglo al contenido ilícito[52], esta no deja de ser una restricción adicional al ámbito de actuación del órgano en cuestión.

Junto con lo anterior, se señala que solo podrán interponer reclamaciones los usuarios digitales establecidos en un Estado miembro de la UE.

---

51. En sus reglas de procedimiento, el órgano expresamente rechaza conocer de disputas relacionadas con contenidos potencialmente ilícitos: "*Content posted may also be illegal. The legality of content posted on platforms cannot be raised to the appeals centre*".
52. ORTOLANI, P., "The resolution of content moderation disputes under the Digital Services Act", *op. cit.*, p. 6.

1.5. RTR

El ámbito de conocimiento del órgano austriaco resulta notoriamente amplio. Del art. 2.2 de las Reglas de procedimiento del órgano se deriva que este podrá conocer de las reclamaciones que se efectúen contra cualquier plataforma en línea que se halle bajo el ámbito de aplicación del RSD, y con independencia de que el fundamento de la decisión de moderación de contenidos sea la ilicitud o la contrariedad con los términos y condiciones.

En este caso, no se aclara si el usuario digital reclamante debe estar establecido fuera o dentro de la UE[53]. Al respecto, consideramos que lo más razonable sería hacer aquí extensiva la argumentación vertida con respecto al órgano húngaro, asumiendo que solo los establecidos en la UE podrían interponer reclamaciones.

1.6. ADR Center

Por último, el órgano certificado por el CSSDD italiano cuenta con exactamente el mismo ámbito de actuación que el órgano austriaco inmediatamente anterior. Es decir, la plataforma en línea potencialmente reclamada —que define el art. 1 de las Reglas de ADR Center en los mismos términos que el art. 3.i) RSD— puede ser cualquiera situada bajo el ámbito de aplicación del Reglamento. Asimismo, el usuario digital será todo aquel que tenga su residencia en la UE, extremo que en este caso no hace falta presumir porque sí se exige en el momento de rellenar el formulario de reclamación —aunque no en las normas del procedimiento—.

A su vez, el fundamento de las decisiones de moderación de contenidos puede ser tanto la ilegalidad como la incompatibilidad con los términos y condiciones (art. 2.3 Reglas de ADR Center).

En definitiva, el análisis anterior sirve para poner de manifiesto que los usuarios digitales no podrán interponer su reclamación ante cualquier órgano certificado con arreglo al art. 21 RSD. Por el contrario, es conveniente que conozcan todos los extremos aquí expuestos, para lo cual deberán acudir a las reglas de procedimiento de cada uno de los órganos. Ahora bien, la elección de órgano también dependerá de otro aspecto adicional: la lengua del contenido controvertido y la lengua en la que se desarrollará el procedimiento extrajudicial.

53. Aunque debe reconocerse que positivamente el art. 1.4 de las Reglas de este órgano dejan claro que el usuario digital puede ser cualquiera que utilice los servicios de la plataforma, con independencia de que esté o no registrado.

2. LENGUA DEL PROCEDIMIENTO

El art. 21.3.e) RSD exige que cada órgano de solución extrajudicial resuelva las reclamaciones en al menos una de las veinticuatro lenguas oficiales de la UE. En concreto, los órganos han sido certificados para actuar en distintas lenguas.

Con respecto a ADROIT, encontramos una situación peculiar. Según la página web oficial de la Comisión Europea[54], este podría resolver sus procedimientos en hasta ocho lenguas diferentes, que incluirían el neerlandés, el inglés, el francés, el alemán, el castellano, el portugués, el italiano y el maltés. Sin embargo, si se consultan las Reglas de procedimiento del órgano en cuestión, se indica que "*Correspondence with ADROIT shall be in English*" (art. 4.n.). De hecho, el inglés es la única lengua en la que se puede rellenar el formulario.

Así las cosas, parece que la Comisión Europea está confundiendo las lenguas en las que está disponible la página web del órgano con la lengua en la que realmente llevará a cabo el procedimiento. Sin perjuicio de esta confusión, los procedimientos extrajudiciales que lleve a cabo ADROIT se desarrollarán, en exclusiva, en inglés.

En cualquier caso, sí existe una correspondencia entre las lenguas indicadas por el resto de los órganos certificados y aquellas señaladas por la página web de la Comisión. De este modo, User Rights resolverá los procedimientos tanto en alemán como en inglés, especificando el art. 3.9 de sus Reglas que si el litigio se debe a la ilicitud del contenido el procedimiento se desarrollará en alemán, mientras que, si la disputa ha sido ocasionada por la contrariedad de la información con las condiciones generales de la plataforma, el procedimiento se llevaría a cabo en alemán o inglés, en función de la lengua en que se hubiera redactado el contenido controvertido.

Por su parte, Tanács resolverá en húngaro. Appeals Centre hará lo propio en inglés, francés, alemán, español, italiano o neerlandés —si bien el contenido controvertido puede estar en cualquier idioma[55]—, y el órgano austriaco RTR se comunicará en exclusiva en alemán —si bien su web también está disponible en inglés— (art. 3.3 de sus Reglas).

---

54. https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement, último acceso el 9 de mayo de 2025.
55. Sus Reglas de procedimiento, después de confirmar que el órgano se comunicará en cualquiera de las seis lenguas especificadas, aclara que "*this does not restrict your ability to submit content in other languages*".

Por último, ADR Center desarrollará sus procedimientos en italiano o en inglés, habida cuenta de que en el formulario son las únicas dos lenguas que los usuarios digitales pueden seleccionar para comunicarse con el órgano de solución. Frente a este escenario, pierde sentido que el art. 1 de las Reglas de este órgano lo caractericen insistiendo en que es capaz de llevar a cabo los procedimientos en cualquier lengua oficial de la UE, así como que el art. 3.3.6 del mismo documento permita al usuario elegir la lengua en la que prefiere que se desarrolle el procedimiento. Como ya se ha dicho, el formulario de reclamación permite elegir la lengua de preferencia, pero la respuesta a esta pregunta es de carácter cerrado y tan solo admite dos posibles opciones: inglés o italiano.

La cuestión que queda sin resolver es la lengua en que debe estar redactado el contenido potencialmente ilícito o contrario a las condiciones generales en los procedimientos que se lleven a cabo ante los órganos que no concretan este aspecto: ADROIT, Tanács y RTR. Cualquiera que sea la respuesta a este interrogante, es indiferente la lengua del contenido si el procedimiento no se puede desarrollar en el idioma de preferencia del usuario digital.

En virtud de lo expuesto, se pueden alcanzar dos ideas fundamentales. La primera es que cada órgano seguirá el procedimiento y la comunicación con las partes en una lengua distinta, debiendo el usuario digital tener en cuenta esta circunstancia a la hora de elegir el órgano ante el que interponer la reclamación del art. 21 RSD. La segunda es que, en conjunto, los órganos certificados tan solo resuelven en nueve lenguas oficiales de la UE, quedando las quince restantes sin representación[56].

3. PLAZO PARA INTERPONER LA RECLAMACIÓN

Conforme a lo indicado anteriormente, el art. 21 RSD estipula de manera expresa cuál es el plazo de que disponen los órganos para resolver las reclamaciones (art. 21.4 RSD), pero guarda silencio en torno al plazo para interponerla, que es, precisamente, el que más interesa al usuario digital. Frente a esta laguna, cada órgano ha suplido la ausencia en un sentido distinto.

Empezando por User Rights, sus Reglas de procedimiento no abordan esta cuestión, pero el formulario para interponer la reclamación alerta de que el órgano tan solo podrá conocer de la decisión de moderación de contenidos adoptada por la plataforma si esta se tomó en los últimos seis meses.

56. Estas son búlgaro, checo, croata, danés, eslovaco, esloveno, estonio, finés, griego, irlandés, letón, lituano, polaco, rumano y sueco.

Además, el formulario establece un *dies a quo* distinto según el sentido de la reclamación.

Por una parte, si el usuario digital reclama porque se le ha retirado un contenido, el plazo de 6 meses empieza a contar desde que se le notificó la decisión[57]. Por otra parte, cuando la reclamación se realice porque el usuario quiere que la plataforma adopte medidas contra un contenido publicado por tercero, el formulario de reclamación exige que antes de acudir al art. 21 RSD se haya señalado ("reportado") el contenido a través del sistema de notificación y acción del art. 16 RSD. Es un requisito previo para que el usuario pueda acudir al órgano del art. 21 RSD. Una vez la plataforma comunique al usuario la respuesta negativa a la notificación del art. 16 RSD —en el sentido de no retirar el contenido—, empezará a contar el plazo de 6 meses para poder acudir al art. 21 RSD[58].

En relación con ADROIT, sus Reglas de procedimiento incorporan una disposición en cierto modo relacionada con el plazo de interposición de la reclamación. Esta estipula que la reclamación será inadmisible si "*the Recipient has not submitted the complaint to ADROIT within one year from the date upon which the Recipient submitted the complaint to the Provider*" (art. 3.b.8). De lo anterior se desprende que el plazo para acudir a ADROIT será de un año a contar desde que el usuario digital solicitó a la plataforma la retirada del contenido conforme al sistema de notificación y acción del art. 16 RSD.

En efecto, en la práctica el plazo para interponer la reclamación será inferior al año: primero, la plataforma deberá resolver "*en tiempo oportuno*" la notificación realizada por el usuario solicitando la retirada del contenido controvertido (art. 16.6 RSD), y una vez notifique al usuario digital su decisión de no retirarlo, será cuando este podrá presentar su reclamación a ADROIT, pero el plazo no comenzará a contar en ese momento, sino cuando el usuario realizó la primera reclamación al amparo del art. 16 RSD. Es criticable, entonces, que no se determine el plazo de interposición de la reclamación cuando el objetivo de la misma no es retirar un contenido, sino todo lo contrario.

---

57. El formulario de reclamación reza lo siguiente: "*User Rights can only process your complaint if the action was taken within the last six months. You can usually find the date of the action in the platform's notification*".

58. Las advertencias del formulario en este caso son distintas al anterior: "*Please note: To submit a complaint with User Rights, you must first report the content to the platform. The platform must have decided not to remove the content*." Y "*User Rights can only process your complaint if the notification was received within the last six months. You can usually find the date in the platform's notification*".

Con respecto al órgano Tanács, la estructura su página web dificulta considerablemente la identificación del plazo. Aun así, el NMHH Decree No. 4/2024 (III.21.) on the detailed rules regarding out-of-court dispute settlement bodies establece directrices mínimas sobre este particular en sus arts. 5.5 y 5.6. En concreto, el plazo para interponer la reclamación frente a Tanács deberá ser como mínimo de 6 meses a contar desde la fecha en que se manifestaron las circunstancias que dieron lugar a la iniciación del litigio, debiéndose identificar este momento con la adopción de la decisión de moderación de contenidos. Por el contrario, el citado órgano deberá establecer un plazo mínimo de un año para aquellos supuestos en que el usuario digital legitimado hubiera tenido conocimiento de las circunstancias que dieron lugar al inicio del litigio —decisión de moderación— de forma tardía o directamente fue impedido de realizar la reclamación. Tal y como se ha sugerido, Tanács debe concretar el significado de estas previsiones en sus Reglas de procedimiento.

Más escueto resulta Appeals Centre, cuyas Reglas fijan un plazo único de 6 meses, a contar desde que la plataforma adoptó la decisión sobre el contenido controvertido. Además, no se especifica nada con respecto al carácter obligatorio u optativo del sistema de notificación del art. 16 RSD.

Por su parte, el órgano austriaco RTR fija el plazo en los seis meses siguientes a la decisión adoptada por la plataforma la primera vez que se contactó con ella (art. 3.4 de sus Reglas de procedimiento). Ello significa que el plazo de seis meses comenzará a contar desde que la plataforma resuelve la notificación realizada por el usuario digital conforme al art. 16 RSD. En efecto, el art. 2.6 de las Reglas exige que "Los usuarios deben haber contactado sin éxito con el respectivo proveedor de servicios antes de enviar su solicitud, es decir, no recibieron respuesta o las dos partes en disputa no pudieron llegar a una solución de la disputa".

Por último, nada dice el órgano certificado en Italia (ADR Center) acerca del plazo en cuestión. A este respecto, la solución más lógica sería aplicar un plazo igual o superior al previsto en el art. 20 RSD, habida cuenta de que el usuario digital puede optar indistintamente por resolver su disputa empleando el sistema interno de gestión de reclamaciones del art. 20 RSD o los órganos de solución extrajudicial del art. 21 RSD. En consecuencia, el plazo de interposición de la reclamación debería ser de 6 meses a contar desde que se notifica al usuario afectado este extremo.

En virtud de lo expuesto, los plazos de interposición de reclamaciones frente a los órganos del art. 21 RSD resultan la mayoría de las veces comple-

jos y distintos. El hecho de que los órganos manejen hasta cuatro plazos de reclamación distintos provoca que los usuarios digitales deban necesariamente contemplar este elemento a la hora de decidir el órgano ante el que interponen la reclamación.

4. TERCERO ENCARGADO DE RESOLVER LA DISPUTA

Otro aspecto del procedimiento que resulta llamativo por el dispar enfoque que han adoptado los órganos certificados tiene que ver con la condición del tercero encargado de resolver la disputa. El Reglamento de Servicios Digitales prefiere no particularizar, y en su lugar ha optado por una terminología amplia: emplea el sintagma "órgano certificado de resolución extrajudicial de litigios" cada vez que quiere referirse al tercero que soluciona la controversia.

Por el contrario, este tercero ha recibido calificativos distintos en las diferentes Reglas de procedimiento de cada uno de los órganos. Así, al tercero se le llama "C*ase Decision-Maker*" (art. 2.d. ADROIT), "*arbitrator*" (art. 2 User Rights), "*reviewer*" (Appeals Centre) o "*assessor*" (art. 1 ADR Center). Por su parte, otros órganos prefieren emplear términos globales, haciendo alusión de manera general a la "Junta de Resolución de Disputas" (Tanács) o al "órgano de resolución de controversias" (RTR).

La disparidad anterior llama todavía más la atención desde el momento en que se comprueba que unas Reglas de procedimiento se contradicen con otras. Por ejemplo, las Reglas de funcionamiento de ADR Center estipulan de manera expresa que "*The Assessor may not act: as an arbitrator, mediator*" (art. 15.1 Reglas ADR Center). Pero ya se ha visto que, por ejemplo, User Rights se refiere a este sujeto precisamente como el "*arbitrator*". O incluso dentro de las Reglas de un mismo órgano podemos encontrar definiciones contradictorias de la función del tercero. Siguiendo con el ejemplo de User Rights, al tercero se le otorga la condición de "*arbitrator*", mientras que en el mismo documento se habla de "*conciliation procedure*" (arts. 3 y concordantes).

En definitiva, lo anterior desemboca en una pluralidad de términos potencialmente capaces de confundir al usuario digital, quien, con arreglo a las distintas formas de designar al tercero que resuelve, podría pensar que esta figura cuenta con un rol diferente en cada uno de los órganos. Sin embargo, la realidad es la contraria: todos ellos tienen la misma función, que es determinar, en exclusiva y sin carácter vinculante, si la decisión de

moderación de contenidos adoptada por la plataforma en línea fue o no la correcta[59]. De ahí que la terminología que parece más apropiada para referirse al tercero o al órgano al que pertenece sea la relativa al conciliador o a un procedimiento de conciliación[60].

5. COSTAS Y HONORARIOS

El régimen de costas y honorarios constituye uno de los pocos puntos del procedimiento extrajudicial que regula de modo detallado el art. 21 RSD. Lo hace en su apartado quinto, al que nos remitimos. Frente a este marco, que otorga poco margen de libre concreción a los órganos certificados, estos tan solo cuentan con la libertad —y obligación— de determinar dos aspectos. El primero es decidir si cobrarán a los usuarios digitales reclamantes una tasa por emplear sus servicios, que, en caso de exigir, deberá ser de coste mínimo. El segundo equivale a la cuantificación de los costes de honorarios que cobrarán a las plataformas en línea cuando sean las legitimadas pasivas de sus procedimientos, sin que en ningún caso puedan superar los costes del procedimiento para el órgano de solución.

De nuevo, ambos interrogantes encuentran respuestas divergentes en cada uno de los seis órganos certificados. No obstante, tan solo prestaremos atención al primero de ellos, toda vez que es el único potencialmente capaz de condicionar la elección de órgano por parte del reclamante. Aunque los honorarios que deben satisfacer las plataformas en línea también gozan de una relevancia singular —especialmente desde la perspectiva de

59. Ya se dijo que la doctrina es unánime al confirmar que los órganos certificados al amparo del art. 21 RSD tan solo pueden pronunciarse sobre el carácter más o menos acertado de la decisión de moderación de contenidos adoptada por la plataforma en cuestión. De hecho, así se desprende de las reglas de procedimiento de cinco de los seis órganos. Sin embargo, el caso de ADR Center es peculiar: al rellenar el formulario de reclamación, el reclamante puede señalar el resultado que le gustaría alcanzar tras el procedimiento. En este contexto, el órgano entre los ejemplos que ofrece permite que, además de poder expresar su deseo por obtener la reactivación de su cuenta o el restablecimiento de su contenido, también podría reclamar un "*economic reimbursement*". Se trata de otro aspecto potencialmente capaz de conducir al legitimado activo a confusión: los órganos no pueden otorgar indemnización por daños y perjuicios.

60. Sin perjuicio de ello, muchos órganos establecen la posibilidad de que las partes lleguen a un acuerdo con ayuda del tercero (mediación) antes de que este deba pronunciarse sin carácter vinculante (conciliación). Es el caso de ADROIT (art. 10), Tanács (art. 17.1 Act CIV of 2023 on certain rules regarding Internet intermediary services), User Rights (art. 5.2.a)), RTR (art. 6.2) y ADR Center (art. 6.4). Por el contrario, sobre esta cuestión no se pronuncia Appeals Centre.

las pequeñas y medianas empresas[61]—, estos resultan indiferentes para determinar si los órganos serán capaces de otorgar una tutela eficaz de los usuarios digitales.

Sentado lo anterior, los órganos certificados se muestran divididos con respecto a la decisión de cobrar o no tasa a los usuarios digitales que reclaman. En este sentido, ADROIT (art. 11), User Rights (arts. 2.2 y 4.2 de su Tabla de Costes —*Schedule of Costs*—[62]) y RTR (art. 15.1) han decidido no exigir ningún precio como condición necesaria para la interposición de la reclamación —salvo que actúen de mala fe—. Por el contrario, Tanács, el órgano húngaro, ha establecido una tasa de 3000 florines (que equivalen, aproximadamente, a 7,5 euros), y Appeals Centre y ADR Center[63] han fijado esta cifra en 5 y 10 euros, respectivamente[64]. Ahora bien, en estos dos últimos casos la cuantía dineraria se reintegraría al reclamante si la disputa se devuelve a su favor. Ello ilustra claramente que la tasa que cobran los órganos irlandés e italiano cuentan con una función disuasoria que pretende evitar reclamaciones infundadas[65].

Sin duda alguna, se trata de otro aspecto que deberán conocer los potenciales legitimados activos para poder decidir el órgano ante el que interponen la reclamación.

---

61. Los honorarios fijados por los órganos certificados, que deberán ser satisfechos por las plataformas en línea reclamadas, son notoriamente exhaustivos en algunos casos, y llamativamente simples en otros. Sin entrar en demasiado detalle, el coste medio por procedimiento oscila en función del órgano certificado. ADROIT fija esta cifra en una horquilla entre 206 y 700 euros (apartado C de su *Fee Model*); User Rights concreta un intervalo de 200 a 700 euros (art. 4 de su *Schedule of Fees*); Appeals Center establece un coste mínimo de 95 euros, y RTR exige una cuantía comprendida entre los 50 y los 550 euros con carácter general (art. 5 de sus Tarifas). Por su parte, Tanács concreta un intervalo de coste mínimo entre 120 y 270 euros (art. 24.1 NMHH Decree No. 4/2024 (III.21.) on the detailed rules regarding out-of-court dispute settlement bodies) y, por último, ADR Center no concreta la cuantía, estableciendo tan solo criterios generales de los que esta dependerá. Sin perjuicio de ello, lo anterior pone claramente de relieve un aspecto: el coste de cada procedimiento es excesivo para una pyme que no puede decidir si acudir o no a los órganos del art. 21 RSD, sino que debe hacerlo cuando así lo estime oportuno el usuario reclamante.
62. Este documento puede descargarse a través del siguiente enlace: https://www.user-rights.org/en/how-it-works, último acceso el 9 de mayo de 2025.
63. https://ods.adrcenter.it/en/Tariffe-del-servizio.html, último acceso el 9 de mayo de 2025.
64. En su intento por promover el uso de la plataforma, el órgano Appeals Centre tiene su página web encabezada por la siguiente oferta: "*For a limited time only, there will be no user fee to submit a dispute*".
65. Otra medida incorporada por Appeals Centre con función disuasoria es la necesidad de registrarse en el órgano para poder interponer la queja.

V. PROBLEMAS DETECTADOS Y SOLUCIONES PROPUESTAS

De todo lo expuesto hasta el momento se puede inferir una conclusión clara: aquellos aspectos donde el art. 21 RSD ha otorgado margen a los órganos extrajudiciales para que concreten los aspectos no regulados por el precepto han sido abordados de manera heterogénea. Esta realidad, que ha confirmado los temores augurados por ciertas voces doctrinales[66], suscita como mínimo dos críticas desde la perspectiva del usuario digital.

De un lado, el alcance de los diferentes ámbitos de actuación de los órganos no solo es muy dispar sino, sobre todo, muy restringido. Sin ir más lejos, si quisiera impugnarse una disputa al amparo del art. 21 RSD empleando como lengua el español, tan solo se podría acudir al Appeals Center, que por el momento es el único órgano que resuelve los litigios en esta lengua. Sin embargo, debe recordarse que este órgano ha sido certificado en exclusiva para solucionar disputas relacionadas con Facebook, Tiktok o Youtube, pero no con ninguna otra plataforma adicional. En consecuencia, reclamaciones interpuestas frente a otras plataformas en línea como Instagram no podrían resolverse recurriendo al art. 21 RSD. Ante estas circunstancias, la tutela que pretende ofrecer este precepto devendría ineficaz.

De otro lado, los órganos del art. 21 RSD presentan un auténtico problema relacionado con la publicidad. La principal cuestión que se suscita a este respecto es determinar cuál es la manera en que el usuario digital puede conocer todos los detalles informativos aquí expuestos, que precisamente necesita para decidir ante qué órgano certificado interpone su reclamación.

En esta línea, el art. 21.1 RSD exige que las plataformas en línea velen por que "*la información sobre la posibilidad para el destinatario del servicio de acceder a una resolución extrajudicial de litigios a que se refiere el párrafo primero sea fácilmente accesible en su interfaz en línea, clara y sencilla*". Sin embargo, si en la práctica se decide interponer una reclamación de este tipo, se puede comprobar que las plataformas en línea, incluidas las de muy gran tamaño, no cumplen con dicha obligación, al menos de la forma que podría esperar un usuario digital medio.

A título de ejemplo, en el momento de poder interponer una reclamación con arreglo al art. 21 RSD, la plataforma Instagram se limita a decir que "*To submit a dispute and get more details, you must go to the website of the dispute*

66. CASAROSA, F., "Out-of-court dispute settlement mechanisms for failures in content moderation", *Jipitec,* vol. 14, núm. 3 (2023), pp. 391-402, p. 395.

settlement body that you choose". Dicho de otro modo, es el usuario digital el que, por sí mismo, debe informarse sobre la existencia y el funcionamiento de los órganos certificados, debiendo estudiar asimismo las reglas de procedimiento correspondientes para poder concluir cuáles son los órganos que eventualmente admitirían su reclamación y en qué condiciones.

Por supuesto, la falta de publicidad de los órganos, las diferencias entre sus reglas, y el hecho de que estas estén redactadas la mayoría de las veces en lengua extranjera, conducen a una clara desprotección del usuario digital, quien antes que informarse por sí mismo preferirá dejar su disputa sin resolver. De nuevo, se puede comprobar que el art. 21 RSD constituye un medio de solución ineficaz para proteger a los usuarios digitales frente a las decisiones de moderación de contenidos de las plataformas.

Lejos de constituir una hipótesis pendiente de comprobación, la ineficacia —por el momento— de los órganos extrajudiciales del art. 21 RSD ha podido ser constatada gracias a dos tipos de informes que han sido publicados de forma reciente.

Por una parte, algunos órganos de solución extrajudicial acaban de publicar con arreglo al art. 21.4 RSD sus informes anuales, en los que, entre otros extremos, deben incluir "*el número de litigios que les hayan sido sometidos, la información sobre los resultados de dichos litigios, el tiempo medio necesario para resolverlos y las deficiencias o dificultades encontradas*". Por el momento, el único órgano que ha revelado este informe ha sido Tanács, certificado en Hungría. Según el mismo[67], en el año 2024 tan solo recibió 18 reclamaciones —procedentes de toda la UE— en virtud del art. 21 RSD.

Por otra parte, también algunas plataformas en línea de muy gran tamaño han publicado sus informes de transparencia correspondientes al segundo semestre de 2024 según los arts. 15, 24 y 42 RSD. En este caso, el art. 24.1.a) les obliga a incorporar información sobre "*el número de litigios sometidos a los órganos de resolución extrajudicial de litigios a que se refiere el artículo 21, los resultados de la resolución de los litigios y el tiempo medio necesario para completar los procedimientos de resolución de los litigios, así como el porcentaje de litigios en los que el prestador de la plataforma en línea haya aplicado las decisiones del órgano;*".

A modo ilustrativo, la plataforma Tiktok ha puesto de relieve que en el segundo semestre de 2024 tan solo se interpusieron contra ella 173 recla-

67. Descargable en el siguiente enlace: https://opvt.hu/opvt/eves-jelentesek, último acceso el 9 de mayo de 2025.

maciones con arreglo al art. 21 RSD (Anexo G)[68]. Pese a que en términos absolutos esta cifra pueda causar una impresión positiva, en términos relativos se puede concluir que estas no representan ni tan siquiera un 0,01% de las reclamaciones que potencialmente se podrían haber interpuesto contra Tiktok[69]. En el mismo sentido, resulta revelador que, durante ese mismo semestre, la plataforma LinkedIn tan solo recibiera 23 reclamaciones de acuerdo con el art. 21 RSD (apartado 8 Informe transparencia de LinkedIn[70]).

En definitiva, las cifras anteriores evidencian que los medios de solución extrajudicial del art. 21 RSD cuentan de momento con un uso real muy inferior a su uso potencial. Dicho de otro modo, estos mecanismos no constituyen todavía una vía de tutela eficaz para los usuarios digitales. La pregunta que en este contexto puede y debe plantearse es si es posible acometer alguna mejoría para incrementar el empleo de estos órganos. A tal fin, se proponen tres soluciones.

En primer lugar, resulta innegociable la necesidad de certificar como mínimo un órgano de solución extrajudicial por cada Estado. Esta sería la única manera de garantizar que como mínimo todas las lenguas oficiales de la UE estén representadas y los usuarios digitales puedan acudir a estos órganos con independencia de cuál sea su lengua materna. Asimismo, resultaría oportuno que estos órganos amplíen sus ámbitos de conocimiento a las disputas interpuestas contra cualquier plataforma en línea que esté bajo el ámbito de aplicación personal del RSD, y no solo contra ciertas plataformas en línea de muy gran tamaño.

En segundo lugar, sería igualmente conveniente homogeneizar algunos aspectos del procedimiento que han sido resueltos de manera divergente por los órganos. Debe mencionarse, como mínimo, el plazo para interponer la reclamación y la condición que recibe el tercero. De esta forma podría reducirse la confusión del usuario digital y simplificar el funcionamiento de los órganos, promoviendo su empleo.

---

68. Informe descargable en https://newsroom.tiktok.com/en-eu/digital-services-act-our-fourth-transparency-report-on-content-moderation-in-europe, último acceso el 9 de mayo de 2025.
69. Téngase en cuenta que, durante este mismo periodo de tiempo, el sistema interno de gestión de reclamaciones de Tiktok recibió un total de 3.085.974 reclamaciones. Habida cuenta de que este mecanismo puede ser empleado alternativamente a los órganos del art. 21 RSD, el resultado es que de las más de 3 millones de reclamaciones que podrían haberse interpuesto frente al art. 21 RSD, tan solo se han hecho realidad 173, que representan un 0,0056%.
70. Se puede descargar en https://www.linkedin.com/help/linkedin/answer/a1678508, último acceso el 9 de mayo de 2025.

Por último, bajo el propósito de estimular el acceso a los órganos de solución extrajudicial del art. 21 RSD, resulta imprescindible que se mejore su publicidad entre los usuarios digitales. Desde el momento en que su queja está lista para ser remitida a un órgano del art. 21 RSD, la plataforma en línea en cuestión debería informarles de manera clara sobre la existencia de estos órganos, sobre sus funciones y sobre su procedimiento. Sería idóneo que, para ello, incorporaran un *hyperlink* o enlace directo, como mínimo a la página web oficial de la Comisión, y a ser posible también deberían indicar, de todos los órganos certificados, cuáles de ellos podrían potencialmente conocer de la reclamación.

Cualesquiera que sean las medidas que pretendan adoptarse, en cualquier caso, resulta urgente la necesidad de implementar soluciones que incrementen el uso de los órganos certificados conforme al art. 21 RSD. En este sentido, las discusiones sostenidas actualmente en torno al rol de estos órganos devienen inútiles desde el momento en que no se puede garantizar su empleo.

Habida cuenta de la lentitud característica de la creación de nuevos órganos en la UE, cabe la posibilidad de que un año no constituya un lapso de tiempo suficiente para extraer conclusiones sobre el uso de este precepto —algo paradójico teniendo en cuenta la celeridad propia de los tiempos digitales que corren—. En este sentido, parece que el sistema de solución extrajudicial del art. 21 RSD se está empezando a poner en marcha.

A título de ejemplo, debe mencionarse que, el pasado 22 de abril de 2025, algunos órganos de solución ya certificados se reunieron para crear la "*ODS Network*", una red que ellos mismos definen como una coalición paneuropea de órganos certificados trabajando para poner en marcha el art. 21 RSD[71]. Resulta esperanzador conocer que, en el seno de esta red, se están empezando a discutir extremos como la necesidad de incrementar el conocimiento de los órganos entre los usuarios digitales.

Cualquiera que sea la manera de abordar esta preocupante situación, debe corregirse con urgencia. De lo contrario, el temor es que el escenario actual desemboque en una situación similar a la que vivió la plataforma ODR creada por el Reglamento 524/2013[72], que tras una inversión económica

71. Esta noticia fue publicada en LinkedIn por el órgano certificado ADROIT el pasado 22 de abril de 2025. Se puede acceder a la misma a través del siguiente enlace: https://www.linkedin.com/company/adroit-legal/, último acceso el 29 de abril de 2025.

72. Reglamento (UE) n o 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se

notoriamente elevada ha habido de ser eliminada[73] debido al desconocimiento de la plataforma entre sus potenciales legitimados activos, lo cual explicaba su ínfima frecuencia de uso[74].

BIBLIOGRAFÍA

CASAROSA, F., "Out-of-court dispute settlement mechanisms for failures in content moderation", *Jipitec,* vol. 14, núm. 3 (2023), pp. 391-402.

CASTELLÓ PASTOR, J.J, "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional*, vol. 17, núm. 1 (2025), pp. 308-328.

CASTELLÓ PASTOR, J. J., "Interrelación del reglamento de servicios digitales con el reglamento *platform to business* (P2B): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea", en CASTELLÓ PASTOR, J. J. (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, Navarra, 2024, pp. 361-398.

DE GREGORIO, G., *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022.

FROSIO, G., y GEIGER, C., "Taking fundamental rights seriously in the Digital Services Act's Platform liability regime", *European Law Journal*, vol. 29, núm. 1-2 (2023), pp. 31-77.

HUSOVEC, M., "Certification of Out-of-Court Dispute Settlement Bodies under the Digital Services Act", *SSRN* (2023), pp. 1-12. Versión en línea accesible en: https://ssrn.com/abstract=4501726, último acceso el 9 de mayo de 2025.

---

modifica el Reglamento (CE) n o 2006/2004 y la Directiva 2009/22/CE. *DO núm. L 165 de 18 de junio de 2013.*

73. Reglamento (UE) 2024/3228 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se deroga el Reglamento (UE) n. o 524/2013 y se modifican los Reglamentos (UE) 2017/2394 y (UE) 2018/1724 en lo que respecta a la supresión de la plataforma europea de resolución de litigios en línea. *DO núm. L de 30 de diciembre de 2024.*

74. Para más detalle sobre este particular, consúltese PALAO MORENO, G., "Avances en el sistema de resolución alternativa de litigios de consumo europeo adaptado a las controversias transfronterizas en el mercado digital", *op. cit.*, pp. 67-104.

HUSOVEC, M., "Will the DSA work?: On Money and Effort", en HOBOKEN, J., et al. (eds.), *Putting the DSA into Practice,* Verfassungsbooks, 2023, pp. 19-35. Versión en línea accesible en: https://ssrn.com/abstract=4384266, último acceso el 9 de mayo de 2025.

LLOPIS NADAL, P., "Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales", en HERNÁNDEZ SAINZ, E., MATE SATUÉ, L. C., y ALONSO PÉREZ, M.T. (coords.), *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales*, Colex, A Coruña, 2023, pp. 140-173.

LOI, M., "Making sense of the Digital Services Act. How to define platforms' systemic risks to democracy", *AW AlgorithmWatch gGmbH* (2023), pp. 1-21.

MORAIS CARVALHO, J., ARGA E LIMA, F., y FARINHA, M., "Introduction to the Digital Services Act, Content Moderation and Consumer Protection", *Revista de Direito e Tecnologia,* vol. 3, núm. 1 (2021), pp. 71-104.

ORTOLANI, P., "The resolution of content moderation disputes under the Digital Services Act", *Giustizia Consensuale*, núm. 2 (2022), pp. 1-21.

PALAO MORENO, G., "Avances en el sistema de resolución alternativa de litigios de consumo europeo adaptado a las controversias transfronterizas en el mercado digital", *Revista e-mercatoria*, vol. 23, núm. 2 (2024), pp. 67-104.

PLA ALMENDROS, R., *La solución extrajudicial de disputas transfronterizas en el Reglamento de Servicios Digitales,* Colex, A Coruña, 2025.

QUINTAIS, J. P., APPELMAN, N. y FATHAIGH, R., "Using Terms and Conditions to apply Fundamental Rights to Content Moderation", *German Law Journal,* núm. 24 (2023), pp. 881-911.

WAGNER, G., Y EIDENMÜLLER, H., "Digital Dispute Resolution", *SSRN* (2021), pp. 1-44. Versión en línea accesible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871612, último acceso el 9 de mayo de 2025.

WIMMERS, J., "The out-of-court dispute settlement mechanism in the Digital Services Act. A disservice to its own goals", *Jipitec*, vol. 12, núm. 5 (2021), pp. 381-401.

Capítulo 5

La adaptación a la era digital del marco europeo de resolución alternativa de litigios "RAL" en materia de consumo*

Enrique Fernández Masiá
Prof. Titular de Derecho Internacional Privado
Universidad de Castilla-La Mancha

SUMARIO: I. EL NUEVO PAQUETE DE REFORMA PROPUESTO EN OCTUBRE DE 2023 POR LA COMISIÓN EUROPEA. II. AMPLIACIÓN DEL ÁMBITO DE APLICACIÓN DE LA DIRECTIVA "RAL" DEL 2013: ¿TODOS LOS LITIGIOS QUE AFECTEN A UN DERECHO DEL CONSUMIDOR DEBEN PODER SER RESUELTOS MEDIANTE UN PROCEDIMIENTO "RAL"? III. UN MEJOR ACCESO Y COMPRENSIÓN DE LOS PROCEDIMIENTOS "RAL" POR PARTE DE LOS CONSUMIDORES Y COMERCIANTES. 1. *Potenciación de las funciones de asistencia de la Red de Centros Europeos del Consumidor*. 2. *Supresión de la plataforma de Resolución de Litigios en Línea "RLL" europea*. IV. UNA MAYOR IMPLICACIÓN EN EL SISTEMA "RAL" DE LOS EMPRESARIOS Y COMERCIANTES Y UNA RACIONALIZACIÓN DE SUS COSTES. V. PREOCUPACIÓN POR LOS CONSUMIDORES VULNERABLES EN LOS MERCADOS DIGITALES. VI. MAYOR SIMPLIFICACIÓN Y TRANSPARENCIA DE LOS PROCEDIMIENTOS "RAL". VII. MENORES OBLIGACIONES PARA LAS ENTIDADES "RAL". VIII. INCENTIVAR A LOS MERCADOS EN LÍNEA Y A LAS ASOCIACIONES COMERCIALES DE LA UNIÓN EUROPEA PARA QUE SUS MECANISMOS

* Este trabajo es parte del proyecto "Hacia una transición digital centrada en la persona en la Unión Europea", TED2021-129307A-I00, financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea "NextGenerationEU"/PRTR, del cual el autor es miembro del equipo de investigación. Este capítulo fue remitido por el autor para su publicación el 12 de marzo de 2025.

DE RESOLUCIÓN DE LITIGIOS CON LOS CONSUMIDORES SE AJUSTEN A LOS CRITERIOS DE CALIDAD DE LA DIRECTIVA "RAL" DEL 2013. BIBLIOGRAFÍA.

I. EL NUEVO PAQUETE DE REFORMA PROPUESTO EN OCTUBRE DE 2023 POR LA COMISIÓN EUROPEA

El incremento y generalización de la actividad comercial internacional ha llevado aparejado directamente un aumento considerable en el volumen y complejidad de los litigios generados en el tráfico mercantil transnacional. Entre éstos, la presencia de un consumidor que contrata con una empresa situada en otro Estado es hoy en día un hecho cada vez más frecuente y cotidiano. La importancia creciente de tales casos internacionales es consecuencia de diversos factores sociales y económicos que se ven interconectados.

Entre ellos, ha de destacarse, en primer lugar, como el turismo a escala europea hace que cada vez en mayor medida sean habituales las compras de consumidores en países distintos del de su residencia. Además, es cada vez mayor el número de nacionales del norte de Europa que poseen una segunda residencia y pasan periodos más o menos extensos de tiempo en países del sur de Europa, cuando no han trasladado su centro de vida a estos últimos. También las importantes y decisivas facilidades derivadas de la implantación del mercado único europeo incentivan la presencia de empresas de un país europeo en otros Estados de la Unión Europea, todo ello conjugado con la introducción de la moneda única europea lo que enormemente ha facilitado asimismo la realización de las transacciones comerciales y la comparación de precios. Por último, junto a la importancia que mantienen las ventas realizadas en ferias internacionales o por catálogo, es innegable que el gran desarrollo que viene viviendo Internet permite a los consumidores acceder desde su casa un inmenso mercado virtual (cada vez más y mejor surtido) en el que satisfacer sus demandas sin necesidad de reparar ya tanto en el lugar de localización (a veces, difícilmente precisable) de la empresa suministradora[1].

1. Sobre ello, son tremendamente ilustrativas las palabras de CASTELLÓ PASTOR, J.J., "Competencia judicial internacional y ADR en materia de contratación electrónica o a distancia", en *Derecho de la Contratación Electrónica y Comercio Electrónico en la Unión Europea y en España*, Castelló Pastor, J. J., Guerrero Pérez A. y Martínez Pérez, M. (Dirs.), Valencia, Tirant Lo Blanch, 2021, pp. 668-669: "Cada vez es más frecuente el consumidor digital; esto es, el consumidor que busca ofertas, compara precios y adquiere el producto o servicio en línea (por ejemplo, a través de las páginas web de los fabricantes o de las plataformas digitales, que proporcionan la infraestructura digital para servicios como mercados virtuales, redes sociales, tiendas de aplicaciones y bus-

Este aumento constante de las relaciones de consumo que presentan algún elemento de extranjería, acentuado por el pujante e imparable fenómeno del comercio electrónico, trae consigo un incremento de los problemas y controversias entre las partes y, consecuentemente, un crecimiento tanto cuantitativo como cualitativo del número de litigios en esta materia. Ante los posibles litigios que pueden plantearse en esta relación contractual, los métodos de resolución de aquellos son básicamente dos: a) acudir a los órganos jurisdiccionales estatales o b) recurrir a las vías de resolución alternativa de conflictos[2].

De estas dos opciones que caben al consumidor y, a pesar del régimen privilegiado y favorecedor de las pretensiones del consumidor en materia de competencia judicial internacional contemplado en el Reglamento Bruselas I bis[3], la realidad nos demuestra que la mayoría de los litigios en materia de consumo se caracterizan por una desproporción entre el valor económico del asunto y el coste de su solución judicial. En particular, en

---

cadores) con independencia del lugar en el que se encuentre el comerciante. En efecto, la posibilidad de reservar la habitación de un hotel, el billete de avión, así como la de comprar ropa, libros o la entrada de un concierto o partido de fútbol a golpe de clic ha permitido incrementar el volumen del comercio electrónico transfronterizo, pero también el desafío del legislador en cómo defender los derechos de los consumidores en línea —que están en un Estado distinto del profesional— sin menoscabar el derecho de los empresarios de la economía digital".

2. Sobre esta dicotomía puede verse, FELIU ALVAREZ DE SOTOMAYOR, S., *La contratación internacional por vía electrónica con participación de los consumidores. La elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos*, Granada, Comares, 2006; GOMEZ VALENZUELA, E., *Resolución judicial y extrajudicial de controversias en la contratación electrónica*, La Coruña, Colex, 2023.

3. Reglamento 1215/2012, del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil —conocido como Reglamento de Bruselas I bis— (DOUE L351, de 20 de diciembre de 2012). El objetivo de las normas contempladas en la Sección 4.ª del Título II del Reglamento de Bruselas I bis radica en proteger al consumidor a la hora de fijar la competencia judicial internacional de los tribunales nacionales dentro del espacio judicial europeo, tomando en consideración, de manera primordial, la posición contractualmente débil de consumidor respecto del empresario. Y esta protección procesal se plasma, principalmente, en dos grandes cuestiones: a) evitar sumisiones jurisdiccionales "a la fuerza", en base a los contratos de adhesión en esta materia y b), permitir que los empresarios puedan ser demandados por los consumidores en el lugar del domicilio de éstos últimos. Una idea, esta última, que se ve, además, reforzada por la irrelevancia de donde tenga el profesional su domicilio, novedad incorporada respecto al Reglamento 44/2001. Sobre este régimen, *Vid.* CALVO CARAVACA, A. y CARRASCOSA GONZALEZ, "Contratos internacionales de consumo", en *Tratado Crítico de Derecho Internacional Privado, Vol. VI, Derecho de los Negocios Internacionales II*, Madrid, Edisofer, 2024, pp. 69-98.

el caso de los conflictos transfronterizos, las posibles dificultades ligadas a los procedimientos judiciales pueden disuadir al consumidor de hacer valer efectivamente sus derechos. Es decir, el recurso a la vía judicial trae consigo una serie de lastres como pueden ser el coste de la consulta jurídica a expertos, la larga duración del proceso (debido al colapso judicial que sufren los sistemas jurisdiccionales de algunos países europeos), las molestias derivadas de sus excesivos formalismos, la incertidumbre en cuanto al resultado o la alta cuantía de las tasas judiciales. Además, la subsistencia de las "fronteras jurídicas" en conflictos de consumo internacionales agudiza las deficiencias recién señaladas y genera asimismo problemas específicos, por ejemplo, en materia lingüística.

Por todos los motivos expuestos, progresivamente ha venido cobrando una mayor relevancia y aceptación el recurso a la denominada resolución alternativa de litigios —en adelante, RAL— en esta materia[4]. Con esta noción, extremadamente amplia y compleja de definir, se está aludiendo a un conjunto de métodos de resolución de litigios distintos a los procedimientos judiciales, que se caracterizan por ser una vía más informal, barata y rápida de solución de controversias[5]. Junto a las ventajas evidentes que ofrece a los consumidores, los mecanismos RAL suponen una descarga de trabajo para los tribunales de justicia y deben asimismo ser valorados positivamente desde la perspectiva del propio empresario, para quien una resolución rápida y efectiva de estos problemas es, en definitiva, una forma de poder obtener la confianza (y con ella, posiblemente las presentes y futuras compras) de los consumidores.

Esta idea de la fidelización del comprador a través de la instauración de unos instrumentos RAL efectivos se pone especialmente de manifiesto en materia de operaciones de consumo por medio del comercio electrónico[6],

4. Aunque no sólo se refiere específicamente a los litigios transfronterizos, C. JEREZ DELGADO, confirma como los denominados MASC (medios alternativos de solución de conflictos), son especialmente útiles para los consumidores porque, con frecuencia, las reclamaciones serán de escasa cantidad y aunque no merecerá la pena acudir ante la jurisdicción, quizás si compense dedicar cierto tiempo a negociar una solución o acudir al arbitraje, "Los MASC en el ámbito del Derecho del consumo", *Diario La Ley*, n.º 10260, 3 de diciembre de 2024, p. 2 (se utiliza la versión digital de este trabajo).
5. Sobre ello, por todos, BARONA VILAR. S., *Nociones y principios de las ADR (solución extrajurisdiccional de conflictos)*, Valencia, Tirant lo Blanch, 2018.
6. Claramente lo expone J.I. PAREDES PEREZ, al declarar que "una de las vías que contribuye a consolidar la confianza de los destinatarios en el comercio electrónico es, sin lugar a dudas, el hecho de disponer de un mecanismo efectivo de resolución extrajudicial de controversias, que les ofrezca la certeza y seguridad de que, en caso de una controversia relacionada con el contrato celebrado, pueda obtener la satisfacción

donde los múltiples problemas que pueden surgir en este sector (como por ejemplo, los derivados de la no entrega o de la entrega defectuosa, o de una información errónea o insuficiente sobre el precio o las características del bien o servicio), se han intentado paliar, desde un primer momento, en el marco europeo sin tener que recurrir a los tribunales de justicia[7].

En este sentido, las instituciones europeas, conscientes de que incentivar el conocimiento y utilización de los métodos de resolución alternativa de litigios es un factor fundamental para lograr la confianza de los consumidores y, ante las diferencias existentes sobre el acceso a éstos a la resolución extrajudicial en toda la Unión Europea, subrayadas de forma especialmente intensa en los casos de poder llevar a cabo o no todo el proceso de resolución del litigio en línea[8], adoptaron un primer paquete de medidas legislativas el 21 de mayo de 2013[9], que incluía: 1) en primer lugar, la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que

---

de sus intereses sin suponerles una carga excesiva ni en tiempo ni en dinero", "Las obligaciones de información de los prestadores de servicios de contratación de bienes o servicios por vía electrónica", en *Derecho de la contratación electrónica…*, *op. cit.*, p. 167.

7. La especial atención que se ha mostrado a la resolución de las controversias individuales en este ámbito por parte de las instituciones europeas, apostando claramente por favorecer los medios de resolución alternativos, no debe hacernos olvidar que también se ha prestado un mayor interés en estos últimos años a la regulación de las acciones de carácter colectivo. En este sentido es reseñable la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DOUE L 409, de 4 de diciembre de 2020). Sobre esta última, puede consultarse, MORENO CORDERO, G., "Impacto de las nuevas directrices europeas en las regulaciones españolas sobre protección de los intereses colectivos de los consumidores", en *Justicia digital, mercado y resolución de litigios de consumo: innovaciones en el diseño del acceso a la justicia*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2021, pp. 455-477.

8. Véase sobre esta cuestión, BARRAL VIÑALS, I., "Tecnología y conflictos en la era de Internet: la utilidad de las Online Dispute Resolution"; *Revista Jurídica de Cataluña*, Vol. 115, n.º 1, 2016, pp. 45-69.

9. Ya previamente la Comisión Europea había adoptado dos Recomendaciones sobre esta cuestión. Nos referimos a la Recomendación 98/257/CE de 30 de marzo de 1998, relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de litigios en materia de consumo y a la Recomendación 2001/310/CE de 4 de abril de 2001 de la Comisión Europea relativa a los principios aplicables a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo. En el Considerando 5 de la Directiva de 2013 se llama la atención a que, desafortunadamente, a pesar de estas dos Recomendaciones, los mecanismos de resolución alternativa de litigios no se han establecido correctamente ni funcionan satisfactoriamente en todas las áreas geográficas o sectores empresariales de la Unión Europea.

se modifica el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE (en adelante, Directiva del 2013 sobre resolución alternativa de litigios en materia de consumo)[10], y 2) en segundo lugar, el Reglamento n.º 542/2013 del Parlamento Europeo y del Consejo sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE (Reglamento del 2013 sobre resolución de litigios en línea en materia de consumo —en adelante, Reglamento RLL europeo—)[11].

Desde su adopción, estas dos medidas legislativas se han convertido en las dos piedras angulares sobre las que se ha asentado el marco jurídico de reparación de los consumidores de la Unión Europea a través del sistema de resolución extrajudicial de litigios[12]. En efecto, por una parte, con la Direc-

10. DOUE L 165, de 18 de junio de 2013. La transposición al Derecho español se produjo mediante la Ley 7/2017 de 2 de noviembre, por la que se incorpora al Ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo (BOE n.º 268, de 4 de noviembre de 2017). Sobre esta última, puede consultarse, BARRAL VIÑALS, I., "La resolución extrajudicial de conflictos con consumidores tras la Ley 7/2017: La mediación en consumo y los otros ADRs", en *El sistema de ADR/ODR en conflictos de consumo: aproximación crítica y prospección de futuro*, I. Viola Demestre y V. Pérez Daudí (Coords.), Barcelona, Atelier, 2019, pp. 17-50; ESTEBAN DE LA ROSA, F., "El sistema español de resolución alternativa de litigios de consumo y la nueva Ley 7/2017, de 2 de noviembre", en *La resolución de conflictos de consumo. La adaptación del Derecho español al marco europeo de resolución alternativa (ADR) y en línea (ODR),* F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2018, pp. 81-106; AGÜERO ORTIZ, A. "La transposición de la Directiva 2013/11/UE al Ordenamiento jurídico español a través de la Ley 7/20217 de 2 de noviembre", en *La resolución de conflictos con consumidores: de la mediación a las ODR,* Barral Viñals, I. (Coord.), Madrid, Reus, 2018, pp. 41-74.

11. DOUE L 165, de 18 de junio de 2013. Como complemento de esta normativa, téngase en cuenta el Reglamento de ejecución (UE) 2015/1051 de la Comisión, de 1 de julio de 2015, sobre las modalidades para el ejercicio de las funciones de la plataforma de resolución de litigios en línea, sobre las modalidades del impreso electrónico de reclamación y sobre las modalidades de cooperación entre los puntos de contacto previstos en el Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo sobre resolución de litigios en línea en materia de consumo, DOUE L 171 de 2 de julio de 2015.

12. Sobre estas medidas legislativas, puede verse, ESTEBAN DE LA ROSA, F. y CORTES, P., "Un nuevo Derecho Europeo para la resolución alternativa y en línea de litigios de consumo", en *La protección del consumidor en dos espacios de integración. Una perspectiva de Derecho internacional, europeo y comparado*, F. Esteban de la Rosa (ed.), Valencia, Tirant lo Blanch, 2015, pp. 514-563; CATALÁN CHAMORRO, M.J., *El acceso a la justicia de consumidores: los nuevos instrumentos de ADR y ODR de consumo*, Valencia, Tirant lo Blanch, 2019. El esfuerzo del legislador europeo por contar con un marco jurídico

tiva del 2013 sobre resolución alternativa de litigios en materia de consumo, se pretendía garantizar que los consumidores de la Unión tuviesen acceso a procedimientos de resolución alternativa de litigios de una alta calidad con los que resolver los litigios contractuales derivados de la venta de bienes o la prestación de servicios por parte de comerciantes establecidos en la Unión Europea a consumidores residentes en la Unión Europea.

En este texto europeo se contempló como los procedimientos de resolución alternativa deben estar abiertos a todos los tipos de litigios nacionales y transfronterizos en materia de contratación de consumo dentro de la Unión, y que dichos procedimientos han de ser llevados a cabo por parte de entidades que permitan que dichos procesos reúnan unos requisitos mínimos, especialmente, en relación con la especialización, la independencia e imparcialidad, igualdad, transparencia, justicia, eficacia y rapidez[13]. Además, se impuso a las autoridades nacionales de los Estados miembros de la Unión Europea el desarrollo de funciones de control en la fase de acreditación de las entidades de resolución alternativa de litigios, así como de supervisión durante su funcionamiento[14]. Y con el fin de aumentar la concienciación de los consumidores y fomentar el uso de la RAL, se estableció que los

---

adaptado a la complejidad y a los cambios constantes que rodean actualmente a los litigios en materia de consumo, encuentra un paralelismo en los trabajos que a nivel internacional se han realizado en la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), en donde en su grupo de Trabajo III —Solución de controversias en línea—, se han adoptado en 2017, unas "Notas Técnicas sobre la solución de controversias en línea". Sobre esta última cuestión, puede consultarse, PALAO MORENO, G., "De la contratación comercial electrónica a la incorporación de lo 'electrónico' en la mediación en los trabajos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL)", en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad)*, S. Barona Vilar (ed.), Valencia, Tirant lo Blanch, 2022, pp. 291-311.

13. *Vid.* CUENCA GARCIA, A., "Los principios de transparencia, eficacia, libertad y legalidad en la Directiva 2013/11/UE del Parlamento Europeo y del Consejo de 21 de mayo de 2013, relativa a la resolución alternativa de litigios de consumo, y su incidencia en el sistema de arbitraje de consumo español", en *Los nuevos instrumentos europeos en materia de conciliación, mediación y arbitraje de consumo. Su incidencia en España, Irlanda y el Reino Unido*, G. Palao Moreno (Ed.), Valencia, Tirant lo Blanch, 2016, pp. 37-79; ORDEÑANA GEZURAGA, I., "Sobre la búsqueda de la esencia (eficacia y calidad) de los mecanismos extrajurisdiccionales para la solución del conflicto de consumo en la Unión Europea o sobre su nuevo marco normativo (La Directiva 2013/11/UE y el Reglamento 524/2103", en *La mediación: algunas cuestiones de actualidad*, V. Pardo Iranzo (Dir.), Valencia, Tirant lo Blanch, 205, pp. 153-212.

14. VALBUENA GONZALEZ, F., "La Directiva europea sobre resolución alternativa de litigios (ADR) en materia de consumo", *Justicia: Revista de Derecho Procesal*, n.º 2, 2014, p. 429.

comerciantes deben estar obligados a informar a los consumidores de la posibilidad de resolver sus litigios por vía extrajudicial a través de estos procedimientos de resolución alternativa.

Por su parte, el Reglamento RLL europeo se adoptó con el único fin de establecer la plataforma europea de resolución de litigios en línea, por medio de la cual los consumidores y los comerciantes pudieran someter sus litigios transfronterizos sobre compras en línea a entidades de resolución alternativa[15]. Llamada a convertirse, teóricamente, en la nueva estrella rutilante en el firmamento de los métodos alternativos de resolución de controversias en la Unión Europea en materia de consumo, la plataforma de RLL ha funcionado desde 2016 como una infraestructura digital totalmente multilingüe en la que los consumidores pueden solicitar a los comerciantes en línea la resolución de un litigio acudiendo a una entidad de resolución alternativa.

Sin embargo, y a pesar de que este marco jurídico adoptado en 2013 ha logrado mantener un alto nivel de derechos para los consumidores dentro de la Unión Europea y unas condiciones equitativas para las empresas en todo el mercado único, tanto los informes sobre su aplicación, como los estudios y consultas realizadas en los últimos años, han conducido a la Comisión Europea a plantearse un nuevo diseño de la situación en este ámbito[16].

Por una parte, en relación con la Directiva de 2013 sobre resolución alternativa de litigios en materia de consumo, se han detectado, principalmente, tres grandes problemas generales que es preciso resolver: a) en primer lugar, su adecuación a los mercados digitales, en segundo lugar, b) la escasa participación de las empresas y los consumidores en la resolución

15. DE MIGUEL ASENSIO, P., *Derecho privado de internet*, 6 ed., Cizur Menor, Thomson-Reuters, 2022, p. 1488. Al respecto de su diseño y los requisitos técnicos exigidos, puede consultarse, FRANCO CONFORTI, O.D., "Diseño de una plataforma de resolución de conflictos por medios electrónicos en el ámbito del consumo", en *Justicia digital, mercado y resolución …*, *op. cit.*, pp. 133-158.

16. Se han elaborado dos informes de evaluación por parte de la Comisión europea en 2019 y 2023 sobre la aplicación de la Directiva de 2013 y el Reglamento RLL europeo. Junto con ello, la Comisión llevó a cabo dos consultas públicas en 2022, una retrospectiva y otra prospectiva sobre este marco europeo de RAL. Además, se organizaron diversos talleres de consulta y una mesa redonda en junio de 2022 sobre la resolución alternativa de litigios transfronterizos y se subvencionaron dos estudios en los años 2022 y 2023 sobre el marco europeo existente y sobre las futuras necesidades. Se puede acceder a toda esta documentación en la página web especialmente dedicada a esta cuestión por parte de la Comisión Europea: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/resolve-your-consumer-complaint/alternative-dispute-resolution-consumers_es#revisi%C3%B3n-de-la-directiva-sobre-ral. (último acceso a todas las páginas web citadas el 12 de marzo de 2025).

alternativa de litigios y, por último, c) la falta de una utilización suficiente en el contexto transfronterizo de la resolución alternativa de litigios. En este sentido, especialmente, queremos destacar como se ha puesto de manifiesto la existencia de una las más importantes carencias que el modelo actual presenta, que no es otra, que el bajo nivel de concienciación y comprensión de estos mecanismos RAL por parte de los consumidores, amén de su falta de confianza —sea o no fundamentada—, lo que directamente incide en su escasa utilización y empleo para en la resolución de las controversias en materia de consumo.

Por su parte, a pesar de que, desde su puesta en funcionamiento en 2016, la página web de la plataforma RLL europea ha recibido más de dos millones de visitas por año, el número de asuntos que han sido resueltos a través de ésta no supera los doscientos al año. Este escaso número ha puesto de manifiesto que la utilidad de la plataforma RLL europea era muy limitada, y que, en consecuencia, no era un instrumento eficiente en términos de los costes que suponen su mantenimiento y funcionamiento. Las razones que están detrás de esta escasa utilización de la plataforma RLL europea podrían encontrarse en[17]:

a) En primer lugar, la falta de información sobre la existencia de la plataforma. Aunque se ha exigido, con razón, que el comerciante debe informar al consumidor sobre la plataforma, no se ha hecho nada para garantizar que esta información se proporcione realmente de una manera que fuera fácilmente accesible para el consumidor[18]. En este sentido, habría sido conveniente la posible creación de un logotipo de la Unión Europea, que apareciese en la página de inicio de la web del empresario. Sin esta información, es bastante impro-

17. Estas razones son expuestas por MORAIS CARVALHO, J. y CAMPOS CARVALHO, J., "Online Dispute Resolution Platform. Making European Contract Law more Effective", en *European Contract Law and the Digital Single Market*, A. De Franceschi (ed.), Cambridge, Intersentia, 2016, pp. 245-266. Estos autores ya pronosticaban que, si no se producían cambios significativos en el funcionamiento de la plataforma RLL europea, ésta tendría un triste final como ahora se ha refrendado. En parecidos términos, propugnando cambios sustanciales en el funcionamiento de la plataforma europea también se había manifestado ESTEBAN DE LA ROSA, F., "¿Quo Vadis plataforma europea de resolución de litigios de consumo? Nuevos pasos en la instauración de un acceso universal digital a la justicia alternativa de consumo en Europa", en *Justicia digital, mercado y resolución …*, *op. cit.*, pp. 35-60, especialmente, pp. 53-56. Igualmente, también, CATALÁN CHAMORRO, M J., *El acceso a la justicia…*, *op. cit.*, pp. 329-347.

18. Sobre esta cuestión es ilustrativa la Sentencia del TJUE, de 25 de junio de 2020 (Sala Sexta) en el asunto C-380/19, *Bundesrverband der Verbraucherzentralen und Verbraucherverbände*, (ECLI:EU:C:2020:498).

bable que tanto los consumidores como los profesionales participen en el proyecto.

b) En segundo lugar, la desconfianza mostrada hacia las entidades RAL, pues en la normativa no se les permite contactar directamente con el comerciante para convencerlo de las ventajas de acudir a la RAL, antes de decidir si se acepta o no el procedimiento.

c) Y, en tercer lugar, se critica la falta de flexibilidad de la plataforma, no estando configurada conforme a los sistemas nacionales de RAL que cuentan con mayor éxito. Así, en aquellas situaciones en donde el procedimiento RAL es obligatorio para los comerciantes conforme a una legislación nacional, la plataforma no cuenta con ningún mecanismo que permita continuar el procedimiento sin la cooperación del propio comerciante.

Tomando en consideración lo que acabamos de señalar, y en consonancia con el interés en el desarrollo de un "Mercado Único Digital", la Comisión Europea presentó el 17 de octubre de 2023, una propuesta de revisión del marco europeo de resolución alternativa de litigios en materia de consumo[19], que pivota en torno a tres acciones de distinto calado que buscan una modernización y puesta al día del sistema existente:

1) En primer lugar, la Propuesta de Directiva del Parlamento Europeo y del Consejo, por la que se modifica la Directiva 2013/11/UE, relativa a la resolución alternativa de litigios en materia de consumo, así como las Directivas (UE) 2015/2302 (UE) 2019/2161 y (UE) 2020/1828[20].

2) En segundo lugar, la Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se deroga el Reglamento (UE)

19. Sobre esta propuesta de revisión del marco europeo de resolución alternativa de litigios en materia de consumo, puede verse, PALAO MORENO, G.; "Avances en el sistema de resolución alternativa de litigios de consumo europeo adaptado a las controversias transfronterizas en el mercado digital", *Revista E-MERCATORIA*, Vol. 23, n.º 2, 2024, pp. 67-104; ZABALLOS ZURILLA, M., "Propuesta de Directiva del Parlamento Europeo y del Consejo, por la que se modifica la Directiva 2013/11/UE, relativa a la resolución alternativa de litigios en materia de consumo, así como las Directivas (UE) 2015/2302, (UE) 2019/2161 y (UE) 2020/1828, COM (2023) 649 Final: principales novedades", *Revista CESCO*, n.º 49, 2024, pp. 33-47; MARCOS FRANCISCO, D., "El futuro de la resolución alternativa de litigios de consumo en la Unión Europea y su incidencia en el sistema arbitral de consumo español", *La Ley Mediación y Arbitraje*, n.º 21, 2024, pp. 1-14 (se utiliza la versión digital de este trabajo).

20. COM (2023) 649 final, Bruselas, 17 de octubre de 2023.

n.º 524/2013 y se modifican los Reglamentos (UE) 2017/2394 y (UE) 2108/1724 en lo que respecta a la desaparición de la plataforma europea de resolución de litigios en línea[21].

3) En tercer lugar y, por último, la Recomendación (UE) 2023/2211 de la Comisión, de 17 de octubre de 2023, relativa a los requisitos de calidad de los procedimientos de resolución de litigios ofrecidos por los mercados en línea y las asociaciones empresariales de la Unión[22].

Con estas tres iniciativas se pretende, de acuerdo con la Comisión Europea, que el marco europeo de resolución alternativa de litigios en materia de consumo se adapte a los mercados digitales[23], pueda mejorarse el acceso de los consumidores en los casos de litigios transfronterizos y, sobre todo, simplificar los procedimientos para todas las partes implicadas en una controversia de este tipo[24]. En este sentido, especialmente, se pone de manifiesto como la normativa existente ya no está adaptada a los litigios derivados de las nuevas tendencias en los mercados de consumo[25], y que los consumido-

21. COM (2023) 647 final, Bruselas, 17 de octubre de 2023.
22. DOUE L de 19 de octubre de 2023.
23. Esta misma idea de una necesidad de que exista un alineamiento de los objetivos de la Unión Europea en esta materia con los cambios sufridos en el mercado digital de consumo, en virtud de la importancia que están adquiriendo actores como los mercados y plataformas digitales, así como la aparición de nuevos hábitos de consumo, es puesta especialmente de manifiesto por PALAO MORENO, G., "Avances en el sistema de resolución alternativa…", *op. cit.*, p. 73.
24. En la Propuesta de Directiva, p. 2, se alude literalmente a estos tres objetivos principales al señalar: "los objetivos de la nueva versión de la Directiva sobre RAL son los siguientes: adaptar el marco de RAL a los mercados digitales abarcando explícitamente una amplia gama de derechos de los consumidores de la UE que pueden no estar mencionados explícitamente en los contratos o que se refieren a fases precontractuales; mejorar el uso de la RAL en los litigios transfronterizos mediante una asistencia más personalizada a los consumidores y los comerciantes; simplificar los procedimientos de resolución alternativa en beneficio de todos los agentes, especialmente reduciendo las obligaciones de presentación de información de las entidades de resolución alternativa y las obligaciones de información de los comerciantes, así como animando a estos a que se impliquen más en las reclamaciones de RAL mediante la introducción de la obligación de responder".
25. Así, en la Exposición de Motivos de la Propuesta de Directiva de 17 de octubre de 2023 se señala como "los consumidores de la UE están realizando, de hecho, muchas más compras en línea, incluso a comerciantes de fuera de la UE. Lamentablemente, se ha producido en paralelo una mayor exposición a fenómenos como las prácticas desleales, a través de interfaces en línea, que distorsionan o menoscaban de manera sustancial, ya sea de manera intencionada o imprudente, la capacidad de los destinatarios de estos servicios de elegir o tomar decisiones de forma autónoma e informada

res cada vez más digitalizados y, en consecuencia, con una impronta más internacionalizada, necesitan tener a su disposición de manera urgente y efectiva, procedimientos mucho más eficientes para resolver litigios que cada vez son más complejos y globales.

En nuestra opinión, aun estando de acuerdo sobre que varias de las innovaciones propuestas de manera singular puedan representar un paso hacia delante en la mejora de este marco europeo como señala la Comisión Europea, sin embargo, tal y como veremos, puede también afirmarse que, aunque no pueda hablarse de un paso atrás, si al menos hay que referirse a la posibilidad de haberse iniciado una fase de ralentización en este ámbito con el lanzamiento de este nuevo paquete de medidas, y sobre todo, con la propuesta de eliminar la plataforma RLL europea, que hoy es ya una realidad tras la publicación en el DOUE del 30 de diciembre de 2024 del Reglamento (UE) 2024/3228 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se deroga el Reglamento (UE) n.º 524/2013 y se modifican los Reglamentos (UE) 2017/2394 y (UE) 2108/1724 en lo que respecta a la desaparición de la plataforma europea de resolución de litigios en línea[26]. Teniendo ello presente, de manera general, en las próximas páginas, en este trabajo se analizan los más importantes aspectos novedosos que se incorporan en esta revisión del marco europeo de resolución alternativa de litigios en materia de consumo.

II. AMPLIACIÓN DEL ÁMBITO DE APLICACIÓN DE LA DIRECTIVA "RAL" DEL 2013: ¿TODOS LOS LITIGIOS QUE AFECTEN A UN DERECHO DEL CONSUMIDOR DEBEN PODER SER RESUELTOS MEDIANTE UN PROCEDIMIENTO "RAL"?

Dentro de la Propuesta de Directiva de 17 de octubre de 2023, una de las ideas clave de su nueva normativa consiste en la ampliación del ámbito de aplicación de la Directiva del 2013 sobre resolución alternativa de litigios en

(interfaces engañosas), la publicidad encubierta, las reseñas falsas, las representaciones distorsionadas de los precios o las falta de información precontractual importante. Estas tendencias también afectan en cierta medida a las compras fuera de línea, ya que los consumidores se ven cada vez más influidos por la comercialización digital, que incide en la afinidad de los consumidores por ciertas marcas y comerciantes específicos. Estas prácticas ponen en peligro la confianza de los consumidores en los mercados digitales y aprovechan la vulnerabilidad de los consumidores".

26. DOUE L de 30 de diciembre de 2024. Sobre esta eliminación, ESTEBAN DE LA ROSA, F., "Cambios en el tratamiento de las reclamaciones transfronterizas motivados por la desactivación de la plataforma europea ODR y la revisión del marco europeo", *La Ley Unión Europea*, n.º 133, febrero, 2025 (se utiliza la versión digital de este trabajo).

materia de consumo, con el fin de adecuarla a la realidad de los mercados digitales. Ante litigios cada vez más complejos, se requieren soluciones más globales y eficientes para que los consumidores puedan hacer valer de una manera efectiva sus derechos.

En esta dirección se proponen diversas modificaciones por parte de la Comisión Europea. Por una parte, respecto de su ámbito de aplicación material, hay que señalar que, en el marco actual, la Directiva del 2013 solamente abarca los litigios relativos a obligaciones contractuales derivadas de contratos de compraventa o de prestación de servicios, entre consumidores residentes en la Unión Europea y comerciantes establecidos en el territorio de la Unión Europea[27]. Con el objetivo de adaptar el marco de RAL a los mercados digitales y fortalecer los derechos de los consumidores a nivel global, la intención de la Comisión Europea es que deben quedar cubiertas todas las categorías de litigios relacionados con los derechos de los consumidores en la Unión Europea[28].

En este sentido, primeramente, deberían abarcarse todos los litigios contra cualquier comerciante que venda bienes o preste servicios, incluidos el contenido digital y los servicios digitales, a consumidores residentes en la Unión Europea. Del mismo modo, también quedarían cubiertos todos los litigios relacionados con las fases precontractuales en las que los consumidores tienen derechos, con independencia de que el consumidor celebre finalmente el contrato o no. En este caso, quedarían cubiertos litigios relacionados con la publicidad engañosa, la falta de información, la información engañosa o poco clara, las cláusulas abusivas o los derechos de garantía. Por otra parte, la ampliación del ámbito de aplicación material tiene también por objeto

27. Este ámbito de aplicación material es calificado por G. PALAO MORENO como tradicional y sensiblemente restrictivo, estando poco adaptado a la realidad de las transacciones y riesgos a los que se enfrentan los consumidores y los usuarios en el contexto de la actual economía digital, "Avances en el sistema de resolución alternativa…", *op. cit.*, p. 80.

28. Como señala la Propuesta de Directiva de 17 de octubre de 2023, "un problema de la Directiva en su versión actual es que su ámbito de aplicación está muy acotado y, por lo tanto, pueden quedar excluidos los litigios relacionados con las fases precontractuales o los derechos de origen normativo, como el derecho a cambiar de prestador de servicios o el derecho a la protección frente al bloqueo geográfico". Con una opinión favorable a esta ampliación del ámbito material se manifiesta M. ZABALLOS ZURILLA, "Propuesta de Directiva del Parlamento Europeo y del Consejo…", *op. cit.*, p. 38, quien no duda en declarar que "es de aplaudir que junto con las obligaciones contractuales derivadas de contratos de compraventa y prestación de servicios se introduzca ahora la posibilidad de acudir también a la RAL cuando los derechos de los consumidores se vean perjudicados en supuestos extracontractuales y precontractuales".

cubrir los litigios relacionados con otros derechos de origen normativo que son importantes para los consumidores, como el derecho a no ser objeto de prácticas de bloqueo geográfico, el derecho a cambiar de empresa de telecomunicaciones o el derecho a acceder a servicios financieros básicos.

En concreto, conforme a lo propuesto por la Comisión el art. 2.1 de la Directiva tendría el siguiente tenor literal: "La presente Directiva se aplicará a los procedimientos de resolución extrajudicial de litigios entre consumidores residentes en la Unión y comerciantes que ofrezcan a dichos consumidores bienes o servicios, incluidos el contenido digital y los servicios digitales, mediante la intervención de una entidad de resolución alternativa de litigios (en lo sucesivo, 'entidad de resolución alternativa'), que propone o impone una solución o que reúne a las partes con el fin de facilitar una solución amistosa en relación con uno de los aspectos siguientes: a) las obligaciones contractuales derivadas de contratos de compraventa, incluido el suministro de contenido digital, o de contratos de prestación de servicios; b) los derechos de los consumidores aplicables a supuestos extracontractuales y precontractuales y contemplados en el Derecho de la Unión en relación con: i) las cláusulas y prácticas comerciales desleales; ii) la información precontractual obligatoria; iii) la no discriminación por razón de la nacionalidad o del lugar de residencia; iv) la posibilidad de recibir servicios y envíos; v) las medidas reparadoras en caso de no conformidad de los productos o del contenido digital; vi) el derecho a cambiar de proveedor; y vii) los derechos de los pasajeros y los viajeros"[29].

Hemos de señalar, sin embargo, que, frente a esta posición expansiva mantenida por parte de la Comisión Europea en su Propuesta de Directiva de octubre de 2023, el Consejo Europeo muestra una posición bastante más contenida en relación con el ámbito de aplicación material que finalmente habría de contemplarse, lo que nos parece más adecuado en función de los fines para los que está diseñado el marco europeo RAL y más acorde con el funcionamiento, estructura y posibilidades de actuación en la actualidad de las entidades[30]. De acuerdo con el mandato de negociación que el Consejo

29. Hay que tener en cuenta que en el texto de la Propuesta se añade que "los Estados miembros también podrán aplicar los procedimientos de resolución alternativa establecidos en la presente Directiva a categorías de litigios distintas de las enumeradas en el párrafo primero, letra b)".

30. Ello está más en consonancia también con lo defendido por parte de las patronales empresariales a nivel europeo una vez conocidas las intenciones de ampliación del ámbito material por parte de la Comisión Europea. En efecto, en este sentido, en la Declaración conjunta emitida el 22 de mayo de 2024 por parte de BusinessEurope, Eurochambres y SME United se señala la innecesariedad de un incremento sustan-

ha adoptado el 25 de septiembre de 2024[31] y, fundamentando su posición en razones de seguridad jurídica y como garantía de una aplicación efectiva del texto europeo, se elimina la posibilidad de acudir a un procedimiento RAL en aquellos supuestos litigiosos que no tengan una naturaleza contractual. Eso sí, entendiendo que dentro de las controversias contractuales se han de incluir también las fases previas a la celebración de un contrato —por ejemplo, la publicidad o el suministro de información— y las posteriores a su finalización —por ejemplo, el uso de contenidos digitales—.

En relación con su ámbito de aplicación territorial, del mismo modo, y frente al régimen contemplado en la Directiva de 2013 que tan solo cubre los litigios que cuenten con un carácter "intracomunitario"[32], la Comisión Europea en su propuesta de Directiva de octubre de 2023, pretende que los comerciantes de terceros países, que ofrecen bienes y servicios, incluidos el

---

tivo del ámbito material de la Directiva de 2013, donde la Propuesta extiende su ámbito a litigios relativos a prácticas no contractuales. Ello puede conducir a que la entidad RAL pudiese intervenir en casos en donde no ha existido un contrato entre el consumidor y el empresario y dichas entidades ni tienen entre su función intervenir en dichos casos ni tampoco están preparadas para ello. En concreto, se afirma que "it is not the role of ADRs to deal with such practices which fall within the remit of national supervisory authorities. The investigation of infringements and breaches of this type require investigative powers that belong solely to those authorities. The spirit of alternative dispute resolution is not to punish nor pursue infringements but to encourage the amicable settlement of disputes arising from the performance of a contract between a professional and a consumer. Adding such powers would require also adding corresponding responsibilities and liabilities for which those bodies that operate ADRs might not be equipped nor motivated to take on board". Esta Declaración conjunta está disponible en: https://www.eurochambres.eu/wp-content/uploads/2024/05/2024-05-22-BusinessEurope-EuroChambres-SME-united-statement-ADR-directive.pdf.

31. "Consumer rights: Council adopts position on measures to facilitate dispute resolution", 25 de septiembre de 2024, disponible en: https://www.consilium.europa.eu/en/press/press-releases/2024/09/25/consumer-rights-council-adopts-position-on-measures-to-facilitate-dispute-resolution/. Previamente ha de tomarse en consideración el Informe sobre la propuesta de Directiva de 26 de febrero de 2024, preparado por la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo (A9-0060/2024), y la posterior Resolución Legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Directiva (P9_TA (2024) 0139), DOUE C, de 27 de febrero de 2025. Respecto a la cuestión del ámbito de aplicación material, ya en el Informe de 26 de febrero de 2024 se había eliminado el numeral vii) del apartado b) del art. 2.1 relativo a los derechos de los pasajeros y viajeros y, en el Resolución de 13 de marzo de 2024, se suprimen los numerales v) y vi).

32. Sobre los criterios de conexión utilizados por la Directiva de 2013 y los problemas interpretativos que pueden plantearse respecto a los mismos, puede consultarse, PALAO MORENO, G., "Avances en el sistema de resolución alternativa…", *op. cit.*, pp. 81-83.

contenido digital y servicios digitales, a consumidores residentes en la Unión Europa, también puedan participar voluntariamente en los procedimientos RAL. Esta nueva idea de ampliación del ámbito de aplicación territorial, en principio, debería ser vista con buenos ojos, como un medio de otorgar un plus de confianza al consumidor europeo en el ámbito del comercio electrónico respecto de comerciantes establecidos fuera de la Unión Europea —no olvidemos que en la práctica una gran parte de las transacciones comerciales en línea se realizan con relación a empresas situadas fuera del territorio europeo—. Sin embargo, puede plantear ciertas dificultades, a la hora de que la entidad RAL haya de contactar con el comerciante establecido fuera de la Unión, así como para poder gestionar eficaz y eficientemente el procedimiento, especialmente por razones de idioma.

La ampliación del ámbito territorial tendría que llevar aparejado una modificación de la definición de que debe entenderse por litigio "transfronterizo", con el fin de abarcar también todos los asuntos en que el comerciante o empresario esté situado fuera de la Unión. En este sentido, por "litigio transfronterizo" habría de entenderse "todo litigio …. en el que el consumidor tenga su residencia en un Estado miembro distinto del Estado miembro en el que esté establecido el comerciante o en el que el consumidor tenga su residencia en un Estado miembro y el comerciante esté establecido fuera de la Unión"[33]. Del mismo modo, también obligaría a los Estados miembros a que garanticen la existencia de entidades de resolución alternativa de litigios que cumplan los requisitos de la Directiva sobre RAL y que tengan competencia para resolver los litigios entre consumidores establecidos en sus territorios y comerciantes de fuera de la Unión Europea.

Las dificultades descritas parecen haber pesado de una manera muy relevante en la posición contemplada en el mandato de negociación del Consejo Europeo de septiembre de 2024. En efecto, la ambición mostrada por parte de la Comisión Europea en su Propuesta de Directiva también se ve limitada respecto a esta importante cuestión. El Consejo estima que deberían ser los Estados miembros los que han de decidir en sus respectivas legislaciones nacionales sobre la aplicación de los procedimientos RAL a los litigios con comerciantes establecidos en terceros países. Con esta decisión se buscaría preservar la eficacia y el funcionamiento práctico del sistema, al mismo tiempo que se quiere evitar una carga administrativa y financiera desproporcionada para los organismos RAL.

33. Art. 4.1 f) de la Propuesta de Directiva de octubre de 2023.

III. UN MEJOR ACCESO Y COMPRENSIÓN DE LOS PROCEDIMIENTOS "RAL" POR PARTE DE LOS CONSUMIDORES Y COMERCIANTES

1. POTENCIACIÓN DE LAS FUNCIONES DE ASISTENCIA DE LA RED DE CENTROS EUROPEOS DEL CONSUMIDOR

Como ya hemos señalado, la preocupación dentro de las instituciones europeas sobre la falta de información y de acceso a los procedimientos RAL por parte de los consumidores dentro de la Unión Europea, especialmente en los casos de litigios transfronterizos, es un motivo esencial para intentar modernizar y simplificar el marco europeo. Y para dar respuesta a estas preocupaciones, especialmente una mejora en la asistencia al consumidor como también, a los propios comerciantes, uno de los vectores que va a guiar la nueva normativa es la pretendida potenciación de las funciones de asistencia e información de los organismos que forman parte de la Red de Centros Europeos del Consumidor (ECC-Net)[34]. No en vano, en las reuniones mantenidas con las distintas partes interesadas, se había puesto de manifiesto la relevancia alcanzada por parte de estos Centros Europeos del Consumidor en la asistencia de los consumidores en relación con los problemas planteados en sus compraventas transfronterizas y cómo sería muy positivo para una resolución eficiente y rápida de los litigios transfronterizos a través de la vía extrajudicial, potenciar en un futuro las funciones de asistencia y asesoramiento de esta Red europea.

En este sentido, se busca mejorar la asistencia específica al consumidor sobre todo lo relacionado con los procedimientos RAL tanto en litigios nacionales[35] como, especialmente, transfronterizos, con el fin de que se pueda comprender como funcionan y se incentive su acceso, al mismo tiempo que se puedan agilizar este tipo de procedimientos[36]. Ha de ofrecerse un apoyo personalizado para ayudar a los consumidores, especialmente a los vulne-

34. Coincidimos con la valoración realizada por ZABALLOS ZURILLA, M., "Propuesta de Directiva del Parlamento Europeo y del Consejo…", *op. cit.*, p. 46, con que esta medida podría convertirse en clave para un impulso decidido de la RAL transfronteriza.

35. Aunque en principio, la asistencia de estos puntos de contacto está pensada para los litigios transfronterizos, la propuesta de Directiva de 17 de octubre de 2023 señala la posibilidad de que los Estados miembros puedan facultar a estos puntos de contacto de resolución alternativa de litigios para prestar asistencia a los consumidores y comerciantes cuando accedan a entidades de resolución alternativa en relación con litigios nacionales.

36. ZABALLOS ZURILLA, M., "Propuesta de Directiva del Parlamento Europeo y del Consejo…", *op. cit.*, p. 43; ESTEBAN DE LA ROSA, F., "Cambios en el tratamiento de las reclamaciones transfronterizas…", *op. cit.*, p. 3.

rables, para gestionar sus reclamaciones y acceder a la entidad o entidades de resolución alternativa competentes más adecuadas para intervenir en su litigio[37]. Deberá ofrecerse asistencia para ayudarles con la traducción de los textos, con el funcionamiento del procedimiento, con las tasas o con la documentación a presentar[38]. Incidiendo, además, en esta idea de potenciación de ayuda a los consumidores, la Resolución del Parlamento Europeo de 13 de marzo de 2024 incorpora la obligación de que los Estados miembros han de garantizar que los consumidores puedan llevar a cabo los procedimientos transfronterizos de resolución alternativa en un idioma oficial del Estado miembro en el que residan.

En esta misma dirección, se obliga a los Estados miembros a la designación de puntos de contacto para realizar este tipo de funciones, preferiblemente, a través de los organismos que forman parte de la Red Europea de Centros Europeos del Consumidor. En concreto, en el art. 14.2 de la Propuesta de Directiva de 17 de octubre de 2023, se prevé como los Estados miembros de la Unión Europea habrán de designar a un centro adscrito a la Red de Centros Europeos del Consumidor, y cuando ello no sea posible, a una organización de consumidores u otro organismo como puntos de contacto de la RAL[39], para prestar ayuda para la presentación de la reclamación, y en su caso la documentación pertinente, facilitar la comunicación entre las partes y la entidad de resolución alternativa competente, asistir en el proceso, proporcionar a las partes y a las entidades de RAL información

37. Incide en esta idea PALAO MORENO, G., "Avances en el sistema de resolución alternativa…", *op. cit*., p. 94, especialmente en relación con los litigios que se pudieran suscitar entre los consumidores que residiesen en un Estado miembro de la Unión Europea y los comerciantes establecidos fuera de la Unión Europea, por razón de su complejidad y la necesidad de garantizar su celeridad y el respeto de sus derechos.

38. Sobre la asistencia y funciones que ya presta en la actualidad el Centro Europeo del Consumidor en nuestro país, en relación con la resolución alternativa de litigios de consumo, puede consultarse, PAREDES PEREZ, J.J., "La participación del Centro Europeo del Consumidor en España en la resolución de litigios transfronterizos de consumo. ¿cambio de funciones? o ¿nuevas funciones?", en *La resolución de conflictos de consumo…*, *op. cit*., pp. 395-413. También es recomendable visitar la página web del propio Centro Europeo del Consumidor en España, donde se informa sobre las funciones encomendadas y se facilita la posibilidad de reclamación por parte de los consumidores españoles respecto a litigios contractuales con empresarios de otros Estados de la Unión Europea, disponible en: https://portal-cec.consumo.gob.es/es.

39. Conforme a lo señalado en el Cdo. 15 de la Propuesta de Directiva de octubre de 2023: "Los Centros Europeos del Consumidor son idóneos para desempeñar estas funciones, ya que están especializados en ayudar a los consumidores en cuestiones relacionadas con sus compras transfronterizas, pero los Estados miembros también deben poder elegir otros organismos especializados pertinentes".

general sobre los derechos de los consumidores de la UE y sobre las normas de procedimiento que aplican las distintas entidades de RAL específicamente, e informar a la parte reclamante de otras vías de recurso cuando un litigio no pueda resolverse mediante un procedimiento de RAL. Una vez designados, se precisa la obligatoriedad de comunicar por parte de los Estados miembros a la Comisión Europea, conforme al art. 24.4, en un plazo determinado tras la entrada en vigor de la modificación de la Directiva, los nombres y las señas de los puntos de contacto de resolución alternativa de litigios que se nombren.

2. SUPRESIÓN DE LA PLATAFORMA DE RESOLUCIÓN DE LITIGIOS EN LÍNEA "RLL" EUROPEA

La idea clave que consideramos que debe presidir la resolución de los litigios en línea es contar con herramientas digitales fáciles de usar para ayudar a los consumidores a encontrar un mecanismo barato, sencillo y simple de reparación en sus litigios transfronterizos[40]. Si bien ésta era también la pretendida vocación con la que se creó la plataforma de RLL europea, la práctica posterior nos ha mostrado que estaba lejos de lograr dicho fin[41]. Como ya hemos señalado, su utilización ha sido más bien escasa por parte de los consumidores, con lo que, tras una evaluación comparativa de los costes asociados a su funcionamiento y los beneficios derivados de su mantenimiento en uso, la Comisión Europea propuso el cierre de la plataforma de RLL europea en la Propuesta de Reglamento de octubre de 2023[42], lo que

40. Aunque se refiera de manera general a la resolución de todo tipo de litigios en materia de consumo, esta idea es apoyada por parte de D. CARRIZO AGUADO, cuando señala que "la eficiencia de un Derecho protector hacia el consumidor se debe medir no por la perfección o equidad de las normas, sino por la existencia de medios asequibles y con escaso coste económica través de los cuales éstos puedan hacer exigibles sus derechos cuando no hayan sido respetados adecuadamente", "Asistencia extrajudicial al consumidor transfronterizo europeo", *Cuadernos de Derecho Transnacional*, Vol. 10, n.º 1, 2018, p. 69.

41. Así se constata en el Informe de evaluación del año 2023 sobre la aplicación de la Directiva de 2013 y el Reglamento sobre RLL europeo. *Vid.* sobre esta cuestión, CATALÁN CHAMORRO, M.J., "Una plataforma de ODR europea, ¿una solución?", en *Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI*, S. Barona Vilar (ed.), Santiago de Chile, Universidad Autónoma de Chile, 2023, pp. 357-376.

42. En este sentido, en la Exposición de motivos de la Propuesta de Reglamento de octubre de 2023 se señala que "a pesar del elevado número de visitas que registra, la plataforma de RLL solo está posibilitando un promedio de 200 asuntos en toda la UE por entidad de resolución alternativa al año. Estos resultados no justifican el coste que supone para la Comisión el mantenimiento de esta herramienta, ni el coste que supone para las administraciones públicas y las empresas en línea el cumplimiento de las obligaciones que les impone el Reglamento sobre RLL. El objetivo de la presente

ha sido confirmado mediante el Reglamento 2024/3228 de 19 de diciembre de 2024[43]. Con ello, además, desaparece la obligación que recaía sobre las empresas en línea de ofrecer un enlace a dicha plataforma, así como también de administrar una dirección electrónica para que se pudieran poner en contacto con ellas.

Un cierre que, en términos absolutos, tendrá poca incidencia sobre las cifras de uso del marco europeo de RAL en materia de consumo —su baja utilización durante los últimos ocho años no puede llevar a engaños—, pero que, desde un punto de vista simbólico, y como ya hemos apuntado, muestra una cierta ralentización en el impulso decidido a los métodos extrajudiciales de resolución de controversias por parte de las instituciones europeas en este ámbito, aunque también hemos de resaltar que es digno de valorar la valentía de aquellas de haberse dado cuenta de que si algo no funciona es mejor cerrarlo y buscar otras opciones más viables y verdaderamente útiles para los consumidores europeos.

Un cierre que se producirá de manera definitiva a partir del 20 de julio de 2025, conforme a lo establecido en el art. 1 del Reglamento 2024/3228 de 19 de diciembre de 2024, donde se suprimirá en esa fecha, toda la información, incluidos los datos personales, relativa a los asuntos sometidos a la plataforma RLL europea. Se ha contemplado, para que la decisión de desactivar la plataforma pueda producirse de manera fluida y sin generar daños[44] que, conforme a los apartados 2 y 3 del art. 2 del Reglamento 2024/3228, no se pueden presentar más reclamaciones ante la plataforma RLL europea a partir del 20 de marzo de 2025, aunque, no obstante, se prevé como la Comisión ha de informar de la supresión de la plataforma a los usuarios que tengan asuntos pendientes antes de esa fecha del 20 de marzo de 2025, ofreciéndoles ayuda para recuperar, si así lo desean, los datos relativos a sus asuntos a los que tengan derecho de acceso.

Pero esta desaparición de la plataforma RLL europea no puede, de ningún modo, suponer una desatención de los consumidores en las situaciones

---

propuesta es, por tanto, derogar el Reglamento sobre RLL, de modo que desaparezca la plataforma de RLL". En un sentido similar los considerandos 4 y 5 del Reglamento 2024/3228, de 19 de diciembre de 2024.

43. Lamenta esta decisión del cierre de la plataforma RLL europea MARCOS FRANCISCO, D., "El futuro de la resolución alternativa de litigios…", *op. cit.*, p. 4, para quién podría haberse reformulado y corregido el funcionamiento de la plataforma para que fuera una verdadera vía de resolución de conflictos online con un servicio de traducción incluido.

44. ESTEBAN DE LA ROSA, F., "Cambios en el tratamiento de las reclamaciones transfronterizas…", *op. cit.*, p. 2.

litigiosas de naturaleza transfronteriza[45]. Y en este sentido, la idea de la Comisión Europea consiste en que la plataforma RLL europea habrá de ser sustituida por una herramienta digital interactiva fácil de usar, que dirigirá y orientará a los consumidores hacia soluciones de recurso destinadas a ellos, garantizando que las personas que busquen información sobre cómo resolver un litigio en materia de consumo puedan obtener rápidamente una respuesta sobre la mejor entidad de resolución alternativa a la que dirigirse en su caso. Así, en concreto, se señala en la propuesta de Directiva que en el artículo 20 de la Directiva de 2013, se añade el apartado siguiente: "8. La Comisión desarrollará y mantendrá una herramienta digital interactiva que proporcione información de carácter general sobre las vías de recurso a disposición de los consumidores y enlaces a las páginas web de las entidades de resolución alternativa que le hayan sido notificadas a efectos del apartado 2 del presente artículo".

Con ello se quiere poner realmente en valor uno de los pocos aspectos que tiene que sobrevivir en relación con el contenido y funcionamiento de la plataforma RLL europea: la plataforma RLL europea como fuente de información relevante. En este sentido, la plataforma siempre ha proporcionado información sobre las entidades RAL[46] y también puede encontrarse información general sobre los procedimientos RAL. Dicha función había sido altamente valorada por las distintas partes interesadas en las consultas realizadas y ha sido tomada en consideración por parte de la Comisión Europea como un medio para lograr una mayor comprensión y una mejora en el acceso a la resolución extrajudicial de litigios en este ámbito. En este sentido, por tanto, la nueva herramienta digital habrá de integrar la lista multilingüe existente de entidades de resolución alternativa en este ámbito, proporcionando soluciones interactivas con las que los consumidores puedan buscar las más adecuadas entidades de resolución alternativa para sus litigios. Y, además, esta nueva herramienta digital también deberá ofrecer información sobre las restantes vías de recurso, incorporando también los enlaces a los nuevos puntos de contacto de resolución alternativa de litigios.

Conforme a lo dispuesto en el mandato de negociación por parte del Consejo Europeo en septiembre de 2024, la Comisión estará obligada a promover esta herramienta digital interactiva, así como a facilitar su manteni-

45. Comparte esta idea PALAO MORENO, G., "Avances en el sistema de resolución alternativa…", *op. cit.*, p. 89.

46. Conforme al art. 20.4 de la Directiva del 2013 sobre resolución alternativa de litigios en materia de consumo, que exige a la Comisión Europea que publique la lista de entidades de resolución alternativa acreditadas.

miento técnico. Además, de acuerdo con el mandato del Consejo se establece un plazo de tres meses a partir de la entrada en vigor de la Directiva RAL revisada para que la Comisión Europea desarrolle íntegramente esta herramienta digital.

IV. UNA MAYOR IMPLICACIÓN EN EL SISTEMA "RAL" DE LOS EMPRESARIOS Y COMERCIANTES Y UNA RACIONALIZACIÓN DE SUS COSTES

La Directiva del 2013 sobre resolución alternativa de litigios en materia de consumo estableció que la participación de los comerciantes y empresarios en los procedimientos RAL debía ser voluntaria, a salvo de lo que pudiera disponer la legislación nacional o una legislación sectorial europea —conforme a su aproximación legislativa de mínimos—. Esta misma idea de voluntariedad no se cambia en la Propuesta de octubre de 2023[47] y, por tanto, las empresas siguen siendo libres para decidir si participan o no en la resolución extrajudicial de litigios, pero también se ha de tomar en consideración que uno de los objetivos principales de la reforma emprendida consiste en impulsar y buscar una mayor implicación en el sistema RAL por parte de los empresarios y comerciantes[48], al mismo tiempo que se pretende garantizar que los procedimientos RAL sean rápidos y se desarrollen en un tiempo oportuno.

En este sentido, en la Propuesta de Directiva de octubre de 2023, se considera obligada la respuesta por parte del empresario a la solicitud de una entidad RAL sobre su intención o no de participar en un procedimiento de este tipo, una vez iniciado por parte de un consumidor, la cual habrá de facilitarse en un plazo razonable, que nunca habrá de superar los veinte días hábiles[49]. Con la incorporación de esta regla, se considera por parte de la

47. Aunque como nos recuerda el Cdo. 13 de la Propuesta de Directiva, la Directiva de 2013 permite que los Estados miembros pueden aprobar normas nacionales para hacer obligatoria la participación de los comerciantes en la RAL en los sectores que consideren adecuados, además de la existencia de la normativa sectorial específica de la Unión Europa que contempla la participación obligatoria de esos comerciantes sectoriales en el sistema RAL.

48. A. BIARD declara que esta falta de implicación y escepticismo puede deberse a que, en algunos de los Estados miembros de la Unión Europea, los comerciantes perciben estos procedimientos RAL como faltos de imparcialidad y proclives a los intereses de los consumidores, "The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking?", *European Journal of Risk Regulation*, Vol. 15, n.º 3, 2024, pp. 633-634.

49. Conforme al mandato de negociación del Consejo Europeo de septiembre de 2024, habría de ampliarse ese plazo de respuesta de veinte días a cuarenta días hábiles en

Comisión Europea que el proceso podría acelerarse y, de esta forma animar a los comerciantes y empresarios a participar en el mismo, aunque la eficacia última de esta medida va a depender de cuales sean las consecuencias que, a nivel nacional, si las hay[50], puedan establecerse para los supuestos en los que el comerciante no responda a la solicitud de la entidad RAL[51].

Por otra parte, y teniendo en cuenta los numerosos deberes de información a los que se ven sometidos los comerciantes y empresarios derivados de la normativa de la Unión de Europea y de las legislaciones nacionales[52], se quiere reducir la carga de obligaciones administrativas de información impuestas especialmente al comerciante en este concreto ámbito[53]. Esta iniciativa se encuadra dentro de una iniciativa de mucho mayor calado a nivel general en donde se intentan reducir los requisitos de información para las empresas y las administraciones publicas dentro de la Unión Europea[54].

En este sentido, y conforme al art. 13.3 del Directiva del 2013, se había establecido dentro de la información que se requiere que deben proporcionar los comerciantes a los consumidores que "…en los casos en que no pueda resolverse un litigio entre un consumidor y un comerciante establecidos

caso de litigios complejos o en circunstancias excepcionales. Y, por otra parte, y con el fin de agilizar en cierta medida el procedimiento, se contempla que, tras la expiración del plazo concedido, la entidad RAL puede considerar la ausencia de respuesta como una negativa del comerciante a participar.

50. La falta de previsión de una sanción en el caso de incumplimiento permite afirmar que esta regla, por muy loable que sea su objetivo, se queda en papel mojado. En este sentido, MARCOS FRANCISCO, D., "El futuro de la resolución alternativa de litigios…", *op. cit.*, p. 6.

51. Al respecto, en el Informe de la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo de 22 de febrero de 2024, se propone que los Estados miembros puedan hacer públicos los nombres de los comerciantes que ignoran injusta y sistemáticamente los resultados de los procedimientos RAL, y que se les exija que den explicaciones por escrito a las demás partes en el procedimiento RAL en caso de que no cumplan su decisión.

52. Sobre estos deberes de información, puede consultarse, PAREDES PEREZ, J.I., "Las obligaciones de información de los prestadores de servicios…", *op. cit.*, pp. 62-185.

53. Como declara M. ZABALLOS ZURILLA, "Propuesta de Directiva del Parlamento Europeo y del Consejo…", *op. cit.*, p. 36, la racionalización de las obligaciones de presentación de información, y la reducción de la carga administrativa constituyen una prioridad.

54. Véase en este sentido, la Comunicación de la Comisión al Parlamento Europeo, Al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Paquete de ayudas a las pymes", COM (2023) 535 final, Estrasburgo, de 12 de septiembre de 2023, que dentro del apartado de reducir la carga de notificaciones e informaciones para las pymes, señala específicamente la simplificación de las obligaciones de notificación derivadas de la legislación de la Unión Europea sobre resolución alternativa de litigios en materia de consumo.

en su territorio tras una reclamación presentada directamente por el consumidor al comerciante, el comerciante facilite al consumidor la información contemplada en el apartado 1 en la que especifique si recurrirá a las entidades de resolución alternativa pertinentes para resolver el litigio. Esta información se facilitará en papel o en cualquier otro soporte duradero".

En la Propuesta de Directiva de 17 de octubre de 2023, se elimina esta obligación por la que los comerciantes, en los litigios nacionales, tienen que informar a los consumidores sobre las entidades de resolución alternativa disponibles, cuando no tienen intención de participar en la RAL. Esta supresión de este deber de información puede parecer a primera vista un poco sorprendente, precisamente, porque esta información tenía como objetivo dar a conocer al consumidor el marco de resolución alternativo de litigios en materia de consumo, valorando éste en su elección de compra si el comerciante había optado por la no participación en el sistema como un factor que puede ser diferencial respecto a otros competidores. En consecuencia y, aunque es verdad que va a racionalizar los costes empresariales, no creemos que la misma ni mucho menos, vaya a ser un importante incentivo para aumentar la utilización de los procedimientos RAL en este ámbito.

V. PREOCUPACIÓN POR LOS CONSUMIDORES VULNERABLES EN LOS MERCADOS DIGITALES

Una de las cuestiones básicas que preocupa a la Comisión Europea y que pretende plasmarse en esta reforma, es la consecución de una protección suficiente para los consumidores vulnerables[55]. La protección de los consumidores vulnerables se enmarca como un importante objetivo a lograr dentro de la Nueva Agenda del Consumidor del 2020 en donde se señala especialmente como "los consumidores de edad avanzada y aquellos con discapacidad también necesitan productos y tecnologías de asistencia accesibles que sean compatibles con las tecnologías de uso general. Un enfoque justo y no discriminatorio de la transformación digital debe atender las necesidades de los consumidores de edad avanzada, los consumidores con discapacidad y, de manera más general, las personas 'desconectadas' que pueden estar menos familiarizadas o sentirse menos a gusto con las herramientas digitales y ser más propensas a caer víctimas del fraude"[56].

55. Aprobando esta manera de actuar, se manifiesta ESTEBAN DE LA ROSA, F., "Cambios en el tratamiento de las reclamaciones transfronterizas…", *op. cit.*, p. 2.
56. Comunicación de la Comisión al Parlamento Europeo y al Consejo, Nueva Agenda del Consumidor, Reforzar la resiliencia del consumidor para una recuperación sostenible, COM (2020) 696 final, 13 de noviembre de 2020, p. 19.

Un objetivo que ha de ser valorado de una manera muy favorable y, que ha de llevar consigo la necesidad imprescindible de incorporar salvaguardias para los consumidores vulnerables, aquellos que carecen de capacidades digitales, incluyendo también aquellos que cuentan con distintos niveles de alfabetización digital[57]. Estas personas no solo han visto mermado su nivel de competitividad en un mercado digitalizado, por causa de la falta de competencias tecnológicas, sino también se ven desamparados en el momento de hacer valer sus derechos ante la justicia. Y ello les hace doblemente vulnerables: no solo en cuanto a su acceso al mercado sino también en cuanto a su acceso a unos medios de resolución de controversias justos y equitativos.

Estamos totalmente de acuerdo con que la falta de estas capacidades digitales puede convertirse en un obstáculo insalvable para muchos consumidores a la hora de buscar una solución rápida, eficiente y justa de sus litigios a través del sistema previsto hasta ahora[58], y ello, no puede encontrar nunca justificación de ningún modo, si no se quiere agrandar también en este ámbito, la brecha digital que muchos de los consumidores padecen, al no estar habituados al uso de las herramientas informáticas[59].

Para la consecución de dicho objetivo de fomentar el recurso a estos medios de resolución de controversias a todo tipo de consumidores, y tras un requerimiento general a los Estados miembros para que faciliten el acceso a los consumidores que residan en su territorio a los procedimientos RAL en el ámbito de aplicación de la Directiva[60], se consigna en la Propuesta de

57. Sobre esta cuestión son muy interesantes las reflexiones de CASAROSA, F., "Access to (Digital) Justice: Is There a Place for Vulnerable People in Online Dispute Resolution Mechanisms?", *Journal of European Consumer and Market Law*, Vol. 13, n.º 3, 2024, pp. 126-133, quién, aunque referidas a las plataformas ODR, considera imprescindible que la mismas aborden las necesidades de cada categoría de personas vulnerables, siendo crucial que las plataformas ODR tomen en consideración el tipo de usuarios de sus servicios (en función de los conflictos que abordan) y establezcan un conjunto básico de adaptaciones que puedan mejorar la posibilidad de que los grupos vulnerables utilicen los procedimientos de resolución de disputas en línea.

58. Si bien la Directiva de 2013 no hacía ninguna referencia a esta cuestión, en el Reglamento del 2013 sobre la plataforma RLL europea en su art. 5.1 ya se hacía mención a que "en el desarrollo, el funcionamiento y el mantenimiento de la plataforma de resolución de litigios en línea se velará por el respeto de la intimidad de sus usuarios desde la fase de diseño ('protección de la intimidad mediante el diseño') y porque, en la medida de lo posible, dicha plataforma sea accesible y utilizable por todas las personas, incluidos los usuarios vulnerables ('diseño para todos')".

59. En este mismo sentido se manifiesta ESPLUGUES MOTA, C., "Consumo, Consumidor, Derecho del consumo…Nuevos retos, ¿Nuevas Respuestas?", en *Derecho del consumo y protección del Consumidor Sustentable en la Sociedad Digital del S XXI*, *op. cit.*, pp. 62-63.

60. Art. 5.1 de la Propuesta de Directiva.

Directiva de octubre de 2023, en primer lugar, la utilización de procedimientos RAL digitales a través de herramientas inclusivas y de fácil acceso. Junto con ello, además, se establece que la opción de presentación, comunicación y transmisión de la reclamación y la documentación en línea[61] no sea la exclusiva, pues siempre que se solicite previamente, cabrá la posibilidad de poder presentar y consultar tanto la reclamación como los documentos justificativos necesarios en un formato no digital.

Hay que señalar que, aún a pesar de la valoración altamente positiva de estas medidas para lograr un elevado nivel de protección de los consumidores europeos en este ámbito, también somos conscientes de que estas facilidades para poder acceder a los procedimientos RAL para todos los consumidores, aunque comprensibles teniendo en cuenta las diferentes destrezas digitales, suponen, sin embargo, unas cargas suplementarias que habrán de implementarse necesariamente en el funcionamiento práctico de las entidades RAL.

En esta misma línea de preocupación por asistir y facilitar el acceso a los consumidores, especialmente los considerados como consumidores vulnerables, al sistema de resolución alternativa de litigios en materia de consumo, hemos de poner de manifiesto como, a pesar de que la Comisión Europea alienta la necesidad de que los procedimientos de resolución alternativa han de ser sencillos, los consumidores tienen la posibilidad de contar con la asistencia en dichos procedimientos de un tercero de su elección. Para dotar de especial eficacia a esta asistencia por parte de un tercero al consumidor, el art. 14.5 de la Propuesta de Directiva de octubre de 2023 señala como los Estados miembros deben garantizar que dicha asistencia se preste de buena fe, para que las partes puedan llegar a alcanzar una solución amistosa, facilitando toda la información necesaria al consumidor con total transparencia, en particular en todo lo que respecta a las posibles tarifas exigidas a cambio de dicha asistencia y a las normas de procedimiento aplicables[62].

VI. MAYOR SIMPLIFICACIÓN Y TRANSPARENCIA DE LOS PROCEDIMIENTOS "RAL"

Una idea central del legislador europeo en este ámbito y, con la que estamos absolutamente de acuerdo, estando presente a la hora de reformar

61. Cuando se utilice la presentación en línea de la reclamación y de los documentos justificativos de la misma, ha de quedar constancia de ello.

62. En consonancia con lo exigido en el Cdo.16 de la Propuesta de Directiva que señala que debe garantizarse que el procedimiento ha de desarrollarse con equidad y plena transparencia.

la Directiva de 2013, consiste en lograr procedimientos RAL mucho más transparentes y fáciles de usar para los usuarios e interesados, al compás de una mayor utilización de los medios tecnológicos que puedan permitir procedimientos más modernos y acordes con los nuevos tiempos que nos ha tocado vivir, al mismo tiempo que se buscan reforzar las competencias de las entidades RAL.

En este sentido, es especialmente destacable la posibilidad contemplada de poder agrupar casos que cuenten con elementos similares contra un mismo comerciante, de tal manera que se puedan lograr resultados idénticos para los consumidores que se encuentran en las mismas circunstancias, especialmente, que se hayan visto sometidos a la misma práctica ilegal[63]. De acuerdo con lo previsto en la Propuesta de Directiva de 17 de octubre de 2023, existirá la posibilidad de que las entidades RAL agrupen casos con elementos similares una vez que hayan informado al consumidor de esta opción y se le dé la oportunidad de oponerse a que su litigio se agrupe junto a otros.

Con esta medida singular de acumulación de asuntos, se trata de lograr un sistema de resolución de litigios más flexible y adaptado a las circunstancias de los casos gestionados por las entidades RAL, al mismo tiempo que tiene como objetivo complementario conseguir una mayor eficiencia tanto para las comerciantes como para las propias entidades RAL. Ha de señalarse que, con posterioridad, aun estando de acuerdo con esta idea, el Consejo Europeo en su mandato de negociación de septiembre de 2024, ha intentado ofrecer a los Estados miembros cierta flexibilidad para establecer las condiciones para la agrupación de casos a nivel nacional, de tal manera que se pueda lograr una adaptación a los diferentes sistemas nacionales de tramitación de reclamaciones.

Además, por otra parte, se toma en consideración que, en una gran mayoría de los casos, con el actual estado de la tecnología y el avance de la inteli-

63. En este sentido, más de la mitad de las respuestas a la consulta pública lanzada por parte de la Comisión en el año 2022, afirmaron que sería muy conveniente el incorporar una regla de este tipo para una mayor facilidad en la tramitación de los casos por parte de las entidades implicadas. Hay que recordar que ya en la Directiva de 2013 en su Cdo. 27 se hacía referencia a esta cuestión al señalar que "la presente Directiva no debe constituir un obstáculo para que los Estados miembros mantengan o introduzcan procedimientos de resolución alternativa por los que se tramiten conjuntamente litigios idénticos o similares entre un comerciante y varios consumidores. Deben llevarse a cabo evaluaciones de impacto de las resoluciones extrajudiciales colectivas antes de que tales resoluciones se propongan a escala de la Unión. La existencia de un sistema eficaz de reclamaciones colectivas y un recurso fácil a la resolución alternativa de litigios deben ser complementarios y ambos procedimientos no deben ser excluyentes".

gencia artificial, pudiera ser que el procedimiento RAL y la resolución de éste, se haya llevado a cabo a través de medios automatizados. En tales casos, se ha precisado en la Propuesta de Directiva de octubre de 2023, que las partes tendrán derecho a solicitar que el resultado de la resolución alternativa de litigios sea revisado por una persona física cuando se acredite que el procedimiento se haya llevado a cabo meramente a través de medios automatizados[64]. Dicho de otra manera, si la resolución del litigio se ha llevado a cabo de forma exclusiva mediante medios automatizados, dicha resolución devendrá definitiva, salvo que las partes soliciten su revisión por una persona física especializada.

La regla descrita parece aceptar en mayor medida la utilización de medios automatizados para la resolución del litigio y evidencia una mayor confianza en los mismos, que aquella contemplada en el caso del sistema interno de gestión de reclamaciones prevista en el art. 21 del Reglamento de Servicios Digitales. En este último caso, recordemos, se ha obligado a que las decisiones que se tomen sobre las reclamaciones presentadas en este sistema se adopten bajo la supervisión de personal altamente cualificado, lo que impide la exclusiva resolución de este tipo de controversias mediante únicamente medios automatizados[65].

Por último, hay que hacer mención sobre que, en la reforma contemplada en la Propuesta de Directiva de 17 de octubre de 2023, se sigue manteniendo como regla general que las entidades RAL pueden rechazar llevar a cabo la resolución de un litigio si el consumidor no ha intentado contactar previa-

64. En todo caso, en el mandato de negociación del Consejo Europeo de septiembre de 2024, se ha dejado claro que las entidades siempre tienen que informar previamente a los consumidores cuando se utilicen sistemas automatizados, incluso de los distintos a los considerados sistemas de alto riesgo conforme a lo previsto en el punto 8a) del Anexo III del Reglamento de Inteligencia Artificial, en los procesos de toma de decisiones de la RAL.

65. Señala a este respecto, el Considerando 58 del Reglamento Europeo de Servicios Digitales cómo los resultados de este sistema de tramitación de reclamaciones deben estar sujetos a revisión humana cuando se usen medios automáticos. Aprobando esta obligación de revisión, puede verse, SANTIESTEBAN GALARZA, M., "Garantías frente a la moderación de contenidos en la propuesta de reglamento único de servicios digitales", *Revista CESCO de Derecho del Consumo*, n.º 41, p. 173; LLOPIS NADAL, P., "Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales", en *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales*, E. Hernández Sainz, L.C. Mate Satué y M.T. Alonso Pérez (Dirs.)., A Coruña, Colex, 2023, p. 157, Para una opinión diferente, abogando por apostar en este sistema interno por la utilización exclusiva de la inteligencia artificial en este ámbito, CASTELLÓ PASTOR, J.J., "Mediación en los conflictos derivados de los servicios digitales en la Unión Europea", en *Meditaciones sobre mediación (MED+)*, S. Barona Vilar (ed.), Valencia, Tirant Lo Blanch, 2022, p. 376.

mente con el comerciante para resolverla. Sin embargo, es destacable como de acuerdo a la nueva redacción del artículo 5, apartado 4, letra a), en dicha Propuesta de Directiva se aclara que, tal y como acabamos de señalar, aunque los consumidores están obligado a intentar resolver previamente el litigio bilateralmente con el comerciante, las entidades de resolución alternativa no deben establecer condiciones desproporcionadas en cuanto a cómo debe producirse el contacto con el comerciante antes de poder proceder a la resolución alternativa del litigio. En este sentido, podrían considerarse que entran en este nivel de desproporción, aquellas condiciones como la obligación de utilizar el sistema interno de recurso de la empresa tras un primer intento fallido de comunicación con el servicio de tramitación de reclamaciones o la obligación de demostrar que se ha contactado con una parte específica del servicio posventa de la empresa[66].

VII. MENORES OBLIGACIONES PARA LAS ENTIDADES "RAL"

Una de las cuestiones básicas puestas de manifiesto tanto en los informes de revisión de 2019 y 2023, como en las reuniones llevadas a cabo con los usuarios e interesados, para intentar lograr un mejor funcionamiento del sistema de resolución alternativo de litigios en materia de consumo a nivel europeo, consiste en la necesidad de adoptar una nueva regulación que tenga en cuenta una mayor racionalización en los requisitos de notificación y comunicación exigidos a las entidades RAL. Como idea general, hemos de confirmar que los cambios propuestos que van en esta dirección deben ser valorados de forma altamente positiva, ya que estas entidades, pensamos, deben dedicarse a lo que realmente es su función para la que son creadas que no es otro que la resolución extrajudicial de litigios en materia de consumo, y no convertirse principalmente en centros burocráticos expendedores de documentos y datos.

Así, y con el fin que acabamos de describir de intentar dar una respuesta coherente a esta necesidad de racionalización[67], una primera medida que se propone en la Propuesta de Directiva de octubre de 2023 consiste en modificar la obligación existente relativa a que las entidades RAL deben publicar informes anuales de actividad detallados en sus sitios web. En su lugar, las entidades RAL deberán publicar informes de actividad resumidos cada dos años. Con este cambio de periodicidad de anual a bienal de esta obligación de la publicación de informes, se busca aliviar la carga administrativa y los costes a las entidades RAL. Además, y dentro de las menciones de información relacionada con los litigios resueltos por las entidades RAL en este

66. Cdo. 12 de la Propuesta de Directiva.
67. Conforme al Cdo. 14 de la Propuesta de Directiva.

informe bienal, se elimina la necesidad de incluir la información sobre la cooperación de la entidad en redes de entidades de resolución alternativa que facilitan la resolución de litigios transfronterizos.

En esta misma dirección, en segundo lugar, se buscan reducir los requisitos de información para las entidades RAL. La Comisión Europea propone suprimir el artículo 19, apartado 3, letras f) a h), de la Directiva del 2013, según las cuales las entidades de resolución alternativa deben informar a las autoridades competentes en materia de RAL sobre: a) la evaluación de la eficacia de las redes en materia de RAL, b) la formación dispensada al personal y c) la evaluación de cómo se proponen mejorar sus resultados. Como con la anterior medida, con la eliminación de informar sobre todo este tipo de cuestiones, se pretende reducir la carga administrativa de las entidades de resolución alternativa de litigios y, de esta manera, lo que sería conveniente, trasladar los recursos ahorrados a poder tramitar más litigios o invertirlos en mejoras de la productividad.

De entre las citadas supresiones de información, la eliminación del deber de informar sobre la formación otorgada a las personas que van a gestionar los procedimientos RAL, nos parece que pudiera ser altamente contraproducente ya que podría incidir en la calidad del sistema. No podemos obviar que una alta y completa formación del personal redunda objetivamente en una mejora de la calidad de los procedimientos RAL, por lo que se puede sospechar que, al eliminar el deber de informar sobre esta cuestión, podría tener como efecto reflejo la reducción del tiempo de formación, así como la calidad de ésta y, por lo tanto, degradar igualmente la calidad de los procedimientos administrados por las entidades RAL. No es extraño, por tanto, que en consonancia con lo que aquí propugnamos, en el mandato de negociación del Consejo de 25 de septiembre de 2024, se haya recuperado dicho requisito de información a las autoridades competentes.

VIII. INCENTIVAR A LOS MERCADOS EN LÍNEA Y A LAS ASOCIACIONES COMERCIALES DE LA UNIÓN EUROPEA PARA QUE SUS MECANISMOS DE RESOLUCIÓN DE LITIGIOS CON LOS CONSUMIDORES SE AJUSTEN A LOS CRITERIOS DE CALIDAD DE LA DIRECTIVA "RAL" DEL 2013

Con esta nueva Recomendación (UE) 2023/2211, a los mercados en línea y a las asociaciones comerciales de la Unión Europea que ofrecen sistemas de resolución de litigios, la Comisión Europea les invita a adaptar dichos sistemas a los criterios de calidad, eficiencia y justicia de la Directiva de 2013

sobre RAL. Como la realidad nos muestra actualmente, y cada vez en mayor medida, un número cada vez mayor de consumidores utiliza mercados en línea —online marketplaces— para comprar bienes y servicios, al mismo tiempo que suelen utilizar los procedimientos de resolución de disputas que estos mercados en línea y las asociaciones comerciales brindan como parte de sus servicios, para resolver las posibles controversias que hayan podido surgir con origen en aquellas transacciones[68].

El cada vez mayor ofrecimiento de estos sistemas y mecanismos de RLL y de tramitación de reclamaciones de naturaleza privada por parte de los propios mercados y por las plataformas digitales, en relación con las operaciones relacionadas con la oferta de productos y servicios en línea, es una de las importantes razones que están detrás de la "caída en desgracia" de la plataforma de RLL europea[69]. Estos procedimientos "privados" de resolución de disputas, no están cubiertos por la Directiva RAL de 2013 y, por lo tanto, no se puede verificar que cumplan con las exigencias de justicia, transparencia y calidad impuestas por la normativa europea. Ante esta situación, la Comisión Europea recomienda, en consecuencia, una serie de medidas concretas para garantizar la eficiencia, la equidad y la justicia de los procedimientos diseñados, así como la experiencia, la imparcialidad y la independencia de las personas que los gestionan. En este sentido, por ejemplo, un sistema RAL justo y eficiente, debe ser transparente sobre los diferentes pasos del procedimiento, como también garantizar que los mediadores sean independientes, posean los conocimientos y competencias necesarias, sin incurrir en conflictos de intereses financieros.

Para lograr unos procedimientos eficaces, es preciso que los mismos sean fácilmente accesibles en línea, que no haya obligación de que las partes estén representadas por un tercero, que sean gratuitos en la medida de lo posible, y que queden resueltos en un plazo razonable, no pudiendo superarse, de manera general, los noventa días naturales desde su inicio. Por otra parte, se recomiendan también una serie de cuestiones que deberían informar a los procedimientos para lograr una verdadera equidad, al garantizar el principio de contradicción e igualdad de armas, una correcta notificación

68. PALFI, D., "Internal Dispute Resolution Systems: Do High Promises Come with Higher Expectations?", *Hungarian Journal of Legal Studies*, Vol. 64, n.º 3, 2024, p. 392.

69. Como pone de manifiesto PALAO MORENO, G., "Avances en el sistema de resolución alternativa…", *op. cit.*, pp. 87-88, esta "privatización de la justicia" en este ámbito, ha provocado que se fuese dejando de lado el empleo de la plataforma de RLL europea de modo paulatino, antes incluso de que se hubiera consolidado plenamente su uso. En este mismo sentido, MARCOS FRANCISCO, D., "El futuro de la resolución alternativa de litigios…", *op. cit.*, p. 5.

de los resultados del proceso, la opción de retirarse en cualquier momento del proceso o la posibilidad de poder acudir, en todo caso, ante un órgano jurisdiccional.

Además, se recomienda que, en caso de que utilicen procedimientos automatizados para resolver litigios, esto se hará público y debería otorgarse a las partes litigantes el derecho a solicitar que el resultado sea revisado por una persona física. Igualmente, se debería informar a los consumidores y comerciantes, antes del inicio del procedimiento, de las cuestiones clave y normas que se van a aplicar al mismo. Por último, en la Recomendación (UE) 2023/2211 se establece que se deberían publicar periódicamente informes de autoevaluación, en intervalos no superiores a dos años, sobre la aplicación de los criterios de calidad recomendados.

BIBLIOGRAFÍA

AGÜERO ORTIZ, A. "La transposición de la Directiva 2013/11/UE al Ordenamiento jurídico español a través de la Ley 7/20217 de 2 de noviembre", en *La resolución de conflictos con consumidores: de la mediación a las ODR*, Barral Viñals, I. (Coord.), Madrid, Reus, 2018, pp. 41-74.

BARONA VILAR. S., *Nociones y principios de las ADR (solución extrajurisdiccional de conflictos)*, Valencia, Tirant lo Blanch, 2018.

BARRAL VIÑALS, I., "Tecnología y conflictos en la era de Internet: la utilidad de las Online Dispute Resolution"; *Revista Jurídica de Cataluña*, Vol. 115, n.º 1, 2016, pp. 45-69.

BARRAL VIÑALS, I., "La resolución extrajudicial de conflictos con consumidores tras la Ley 7/2017: La mediación en consumo y los otros ADRs", en *El sistema de ADR/ODR en conflictos de consumo: aproximación crítica y prospección de futuro*, I. Viola Demestre y V. Pérez Daudí (Coords.), Barcelona, Atelier, 2019, pp. 17-50.

BIARD, A., "The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking?", *European Journal of Risk Regulation*, Vol. 15, n.º 3, 2024, pp. 625-636.

CALVO CARAVACA, A. y CARRASCOSA GONZALEZ, "Contratos internacionales de consumo", en *Tratado Crítico de Derecho Internacional Privado, Vol. VI, Derecho de los Negocios Internacionales II*, Madrid, Edisofer, 2024, pp. 69-98.

CARRIZO AGUADO, D., "Asistencia extrajudicial al consumidor transfronterizo europeo", *Cuadernos de Derecho Transnacional*, Vol. 10, n.º 1, 2018, pp. 45-69.

CASAROSA, F., "Access to (Digital) Justice: Is There a Place for Vulnerable People in Online Dispute Resolution Mechanisms?", *Journal of European Consumer and Market Law*, Vol. 13, n.º 3, 2024, pp. 126-133.

CASTELLÓ PASTOR, J.J., "Competencia judicial internacional y ADR en materia de contratación electrónica o a distancia", en *Derecho de la Contratación Electrónica y Comercio Electrónico en la Unión Europea y en España*, Castelló Pastor, J. J., Guerrero Pérez A. y Martínez Pérez, M. (Dirs.), Valencia, Tirant Lo Blanch, 2021, pp. 643-683.

CASTELLÓ PASTOR, J.J., "Mediación en los conflictos derivados de los servicios digitales en la Unión Europea", en *Meditaciones sobre mediación (MED+)*, S. Barona Vilar (ed.), Valencia, Tirant Lo Blanch, 2022, pp. 357-380.

CATALÁN CHAMORRO, M.J., *El acceso a la justicia de consumidores: los nuevos instrumentos de ADR y ODR de consumo*, Valencia, Tirant lo Blanch, 2019.

CATALÁN CHAMORRO, M.J., "Una plataforma de ODR europea, ¿una solución?", en *Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI*, S. Barona Vilar (ed.), Santiago de Chile, Universidad Autónoma de Chile, 2023, pp. 357-376.

CUENCA GARCIA, A., "Los principios de transparencia, eficacia, libertad y legalidad en la Directiva 2013/11/UE del Parlamento Europeo y del Consejo de 21 de mayo de 2013, relativa a la resolución alternativa de litigios de consumo, y su incidencia en el sistema de arbitraje de consumo español", en *Los nuevos instrumentos europeos en materia de conciliación, mediación y arbitraje de consumo. Su incidencia en España, Irlanda y el Reino Unido*, G. Palao Moreno (Ed.), Valencia, Tirant lo Blanch, 2016, pp. 37-79.

DE MIGUEL ASENSIO, P., *Derecho privado de internet*, 6 ed., Cizur Menor, Thomson-Reuters, 2022.

ESPLUGUES MOTA, C., "Consumo, Consumidor, Derecho del consumo… Nuevos retos, ¿Nuevas Respuestas?", en *Derecho del Consumo y Protección del Consumidor Sustentable en la Sociedad Digital del S XXI*, S. Barona Vilar (ed.), Santiago de Chile, Universidad Autónoma de Chile, 2023, pp. 47-66.

ESTEBAN DE LA ROSA, F. y CORTES, P., "Un nuevo Derecho Europeo para la resolución alternativa y en línea de litigios de consumo", en *La pro-*

tección del consumidor en dos espacios de integración. Una perspectiva de Derecho internacional, europeo y comparado, F. Esteban de la Rosa (ed.), Valencia, Tirant lo Blanch, 2015, pp. 514-563.

ESTEBAN DE LA ROSA, F., "El sistema español de resolución alternativa de litigios de consumo y la nueva Ley 7/2017, de 2 de noviembre", en *La resolución de conflictos de consumo. La adaptación del Derecho español al marco europeo de resolución alternativa (ADR) y en línea (ODR)*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2018, pp. 81-106.

ESTEBAN DE LA ROSA, F., "¿Quo Vadis plataforma europea de resolución de litigios de consumo? Nuevos pasos en la instauración de un acceso universal digital a la justicia alternativa de consumo en Europa", en *Justicia digital, mercado y resolución de litigios de consumo: innovaciones en el diseño del acceso a la justicia*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2021, pp. 35-60.

ESTEBAN DE LA ROSA, F., "Cambios en el tratamiento de las reclamaciones transfronterizas motivados por la desactivación de la plataforma europea ODR y la revisión del marco europeo", *La Ley Unión Europea*, n.º 133, febrero, 2025, 5 pp. (se utiliza la versión digital de este trabajo).

FELIU ALVAREZ DE SOTOMAYOR, S., *La contratación internacional por vía electrónica con participación de los consumidores. La elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos*, Granada, Comares, 2006.

FRANCO CONFORTI, O.D., "Diseño de una plataforma de resolución de conflictos por medios electrónicos en el ámbito del consumo", en *Justicia digital, mercado y resolución de litigios de consumo: innovaciones en el diseño del acceso a la justicia*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2021, pp. 133-158.

GOMEZ VALENZUELA, E., *Resolución judicial y extrajudicial de controversias en la contratación electrónica*, La Coruña, Colex, 2023.

JEREZ DELGADO, C., "Los MASC en el ámbito del Derecho del consumo", *Diario La Ley*, n.º 10260, 3 de diciembre de 2024, 14 pp. (se utiliza la versión digital de este trabajo).

LLOPIS NADAL, P., "Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales", en *La responsabilidad civil por servicios de intermediación prestados por plataformas*

digitales, E. Hernández Sainz, L.C. Mate Satué y M.T. Alonso Pérez (Dirs.)., A Coruña, Colex, 2023, pp. 140-173.

MARCOS FRANCISCO, D., "El futuro de la resolución alternativa de litigios de consumo en la Unión Europea y su incidencia en el sistema arbitral de consumo español", *La Ley Mediación y Arbitraje*, n.º 21, 2024, pp. 1-14 (se utiliza la versión digital de este trabajo).

MORAIS CARVALHO, J. y CAMPOS CARVALHO, J., "Online Dispute Resolution Platform. Making European Contract Law more Effective", en *European Contract Law and the Digital Single Market*, A. De Franceschi (ed.), Cambridge, Intersentia, 2016, pp. 245-266.

MORENO CORDERO, G., "Impacto de las nuevas directrices europeas en las regulaciones españolas sobre protección de los intereses colectivos de los consumidores", en *Justicia digital, mercado y resolución de litigios de consumo: innovaciones en el diseño del acceso a la justicia*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2021, pp. 455-477.

ORDEÑANA GEZURAGA, I., "Sobre la búsqueda de la esencia (eficacia y calidad) de los mecanismos extrajurisdiccionales para la solución del conflicto de consumo en la Unión Europea o sobre su nuevo marco normativo (La Directiva 2013/11/UE y el Reglamento 524/2103", en *La mediación: algunas cuestiones de actualidad*, V. Pardo Iranzo (Dir.), Valencia, Tirant lo Blanch, 2015, pp. 153-212.

PALAO MORENO, G., "De la contratación comercial electrónica a la incorporación de lo 'electrónico' en la mediación en los trabajos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL)", en *Justicia poliédrica en período de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad)*, S. Barona Vilar (ed.), Valencia, Tirant lo Blanch, 2022, pp. 291-311.

PALAO MORENO, G.; "Avances en el sistema de resolución alternativa de litigios de consumo europeo adaptado a las controversias transfronterizas en el mercado digital", *Revista E-MERCATORIA*, Vol. 23, n.º 2, 2024, pp. 67-104.

PALFI, D., "Internal Dispute Resolution Systems: Do High Promises Come with Higher Expectations?", *Hungarian Journal of Legal Studies*, Vol. 64, n.º 3, 2024, pp. 391-412.

PAREDES PEREZ, J.J., "La participación del Centro Europeo del Consumidor en España en la resolución de litigios transfronterizos de consumo.

¿cambio de funciones? o ¿nuevas funciones?", en *La resolución de conflictos de consumo. La adaptación del Derecho español al marco europeo de resolución alternativa (ADR) y en línea (ODR)*, F. Esteban de la Rosa (Dir.), Cizur Menor, Thomson-Reuters Aranzadi, 2018, pp. 395-413.

PAREDES PEREZ, J.I., "Las obligaciones de información de los prestadores de servicios de contratación de bienes o servicios por vía electrónica", en *Derecho de la Contratación Electrónica y Comercio Electrónico en la Unión Europea y en España*, Castelló Pastor, J. J., Guerrero Pérez A. y Martínez Pérez, M. (Dirs.), Valencia, Tirant Lo Blanch, 2021, pp. 62-183.

SANTIESTEBAN GALARZA, M., "Garantías frente a la moderación de contenidos en la propuesta de reglamento único de servicios digitales", *Revista CESCO de Derecho del Consumo*, n.º 41, 2022, pp. 158-179.

VALBUENA GONZALEZ, F., "La Directiva europea sobre resolución alternativa de litigios (ADR) en materia de consumo", *Justicia: Revista de Derecho Procesal*, n.º 2, 2014, pp. 409-443.

ZABALLOS ZURILLA, M., "Propuesta de Directiva del Parlamento Europeo y del Consejo, por la que se modifica la Directiva 2013/11/UE, relativa a la resolución alternativa de litigios en materia de consumo, así como las Directivas (UE) 2015/2302 (UE) 2019/2161 y (UE) 2020/1828, COM (2023) 649 Final: principales novedades", *Revista CESCO*, n.º 49, 2024, pp. 33-47.

BLOQUE II

Capítulo 6

Sistemas de Inteligencia Artificial y responsabilidad por productos defectuosos en supuestos transfronterizos: novedades en su regulación europea y régimen conflictual*

Guillermo Palao Moreno
Catedrático de Derecho Internacional Privado
Universitat de Valéncia

SUMARIO: I. INTRODUCCIÓN. II. LA REGULACIÓN EUROPEA DE LA RESPONSABILIDAD CIVIL OCASIONADA POR SISTEMAS DE INTELIGENCIA ARTIFICIAL: ESTADO DE LA CUESTIÓN E IMPACTO EN LA MODERNIZACIÓN DEL RÉGIMEN DE RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS. 1. *Los esfuerzos del legislador europeo por establecer un marco regulatorio en relación con la responsabilidad civil derivada de sistemas de Inteligencia Artificial*. 2. *La Directiva (UE) 2024/2853 sobre responsabilidad por los daños causados por productos defectuosos y su impacto en el ámbito de la Inteligencia Artificial*. III. LA RESPONSABILIDAD POR PRODUCTOS TRANSFRONTERIZA POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL: ASPECTOS DE LEY APLICABLE. 1. *Cuestiones introductorias*. 2. *La problemática que suscita la aplicación del Convenio de La Haya de 1973*. 3. *Las posibilidades que ofrece el Reglamento Roma II*. IV. VALORACIÓN.

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro el autor y del Proyecto Prometeo CIPROM 2023-64 (GV) ("Justicia sostenible en estado de mudanza global"). ORCID: 0000-0002-3267-39. E-mail: Guillermo.palao@uv.es. Todas las páginas web visitadas fueron accedidas por última vez el 30 de mayo de 2025.

I. INTRODUCCIÓN

1. La Inteligencia Artificial (IA) constituye ya una realidad que nos acompaña en muchas de las acciones y decisiones que llevamos a cabo a diario, constituyendo una tecnología disruptiva que ofrece grandes oportunidades y presenta no menos importantes retos al Derecho. Dentro de los riesgos que se relacionan con el empleo y funcionamiento de los sistemas de IA, se sitúan los posibles perjuicios que, en la persona o su patrimonio, podamos sufrir cualquiera de nosotros en el marco de nuestra actividad. En esta línea, se pueden mencionar ejemplos como los eventuales perjuicios que pudieran ocasionarse por vehículos autónomos, por los resultados adversos derivados del empleo de sistemas de IA para realizar diagnósticos médicos o para la toma de decisiones financieras, crediticias o de inversión incorrectas o resultantes de datos defectuosos, al igual que los daños que fueran causados por un robot industrial programado con IA por motivo de una programación, actualización o mejora defectuosa. Unos daños que, desde la perspectiva jurídica, implica el reto de su adecuada disciplina legal; exigiendo la adaptación y modernización de un marco normativo que no se encontraba diseñado para atender a este tipo de situaciones en el momento en que fue concebido.

2. Así las cosas, en el contexto de la conocida como "Estrategia Digital Europea", el legislador de la Unión Europea (UE) se ha preocupado en dotar de un marco regulatorio a la IA que atendiera a los retos legales que suscitaba durante los últimos años. Algo que se ha ido desarrollado de forma paulatina y cuyo primer impulso se puede situar en la publicación por la Comisión de la Comunicación "Inteligencia Artificial para Europa"[1], y la Comunicación "Plan Coordinado sobre Inteligencia Artificial"[2], ambas de 2018. Desde ese momento se han ido sucediendo, a impulso principal de la Comisión, pero también del Parlamento Europeo, distintos documentos que iban sentando las bases de los instrumentos normativos, que se han ido presentando en su versión finalizada desde 2024.

De este modo, por mencionar los más relevantes y por lo que hace a la labor desarrollada por la Comisión, sobresale la elaboración la Comunicación "Generar confianza en la Inteligencia Artificial centrada en el ser humano"[3] y el "Libro Blanco sobre la Inteligencia Artificial — un enfoque europeo orien-

1. COM (2018) 237 final.
2. COM (2018) 795 final. El cual se vería actualizado, con posterioridad, por medio de la Comunicación "Fomentar un planteamiento europeo en materia de inteligencia artificial" (COM (2021) 205 final).
3. COM (2019) 168 final.

tado a la excelencia y la confianza"[4], ambos en 2020. Al igual que, ya en 2021, la publicación de la Comunicación "Fomentar un planteamiento europeo en materia de Inteligencia Artificial"[5], o la revisión del "Plan Coordinado sobre Inteligencia Artificial"[6]. A las que seguirían el "Pacto para la Inteligencia Artificial"[7] y la Comunicación "Impulso a las empresas emergentes y la innovación en inteligencia artificial fiable"[8], de 2024.

3. El resultado regulatorio más relevante y reciente, al respecto de la preocupación europea por el impacto jurídico que posee la incorporación de la IA en el mercado interior, ha sido la publicación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) 300/2008 (UE) 167/2013 (UE) 168/2013 (UE) 2018/858 (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE (UE) 2016/797 y (UE) 2020/1828 (Reglamento de IA)[9]. El Reglamento de IA, por tanto, constituye un relevante instrumento normativo, por medio del que se ofrece una regulación uniforme obligatoria y singularmente estricta para los operadores e intermediarios que actúan en la UE; incorporando, a tal efecto, un sistema de evaluación, acreditación, vigilancia y sancionador de su actividad[10].

El Reglamento de IA se encuentra localizado en el contexto de las llamadas "Leyes digitales", a partir de la cuales se continua con el impulso que supuso el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)[11]; así como acompaña a otros textos relevantes

4. COM (2020) 65 final.
5. COM (2021) 205 final.
6. COM (2021) 206 final.
7. En: https://digital-strategy.ec.europa.eu/es/policies/ai-pact
8. COM (2024) 28 final.
9. *DO L 1689, de 12 de julio de 2024.* En vigor, según dispone su art. 113, desde el 1 de julio de 2024; aunque contemplándose una aplicabilidad plena por tramos, desde el 2 de febrero de 2025 al 2 de agosto de 2027. *Vid.* BARRIO ANDRÉS, M. (Dir.), *El Reglamento europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia (2024); COTINO HUESO, L. y SIMÓN CASTELLANO, P. (Dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Pamplona (2025); ORTEGA GIMÉNEZ, A.: *El Reglamento europeo de inteligencia artificial (IA): Análisis y aplicación práctica*, Sepin, Madrid (2025).
10. ORTEGA GIMÉNEZ, A.: *El Reglamento europeo... opc.it.*, p. 18.
11. *DO* L 119, de 4 mayo de 2016. Con posterioridad sobresalen, la Comunicación "Hacia un espacio común europeo de datos" (COM (2018) 232 final), la Resolución del

para el "Mercado Único Digital" como el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)[12] y el Reglamento (UE) 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)[13].

4. Sin embargo, ese mismo año, tampoco presentaba una relevancia menor la presentación al público de la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo[14]. Un valioso instrumento que, como establece su art. 23, entró en vigor el 28 de noviembre de 2024, aunque estableciendo un plazo de transposición para los Estados miembros hasta el 9 de diciembre de 2026, en su art. 22. La Directiva (UE) 2024/2853 constituye el primer instrumento publicado por la UE en el marco de lo que se conoce como la "Leyes de responsabilidad en materia de IA", por medio del que atiende a objetivo del buen funcionamiento del mercado interior, por medio del establecimiento de un régimen armonizado de responsabilidad civil extracontractual de naturaleza objetiva[15].

Así las cosas, la mencionada Directiva y como se indica en su propio título, viene a reemplazar Directiva 85/374/CEE, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por

---

Parlamento Europeo, sobre una Estrategia Europea de Datos de 2021 (*DO* C 494, de 8 diciembre 2021), que condujo a la publicación del Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento 2018/1724 (*DO* L 152, de 3 junio de 2022) o del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (*DO* L 2023/2854, de 22 de diciembre de 2023).

12. *DO* L 265, de 12 de octubre de 2022.
13. *DO* L 277, de 17 de octubre de 2022. También, el Reglamento de Ejecución (UE) 2023/1201 de la Comisión de 21 de junio de 2023, relativo a las disposiciones detalladas para la tramitación de determinados procedimientos por parte de la Comisión con arreglo al Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo ("Ley de Servicios Digitales"). *DO* L 159, de 22 de junio de 2023.
14. *DO* L 2024/2853, de 18 de noviembre de 2024.
15. Considerandos 1 y 2.

productos defectuosos[16]. La Directiva (UE) 2024/2853 se nos presenta, por consiguiente, como el resultado directo de un esfuerzo modernizador que resultaba necesario, por medio del que se ambiciona atender a la necesidad de contar con un marco regulador acorde a los desafíos que actualmente implican los avances tecnológicos, incluida la IA[17]; desempeñando un papel clave en el contexto de la estrategia europea en materia de responsabilidad civil en relación con la IA[18].

A este respecto y desde la perspectiva del Derecho de la responsabilidad civil, una de las cuestiones que primero interesó a especialistas e instituciones europeas, desde la perspectiva de la IA, se dirigió a determinar si la normativa en materia de productos defectuosos se adaptaba a los daños ocasionados por los sistemas de IA[19]. Una realidad que, en todo caso. precisaban de un correcto tratamiento legal. Pensemos en situaciones como la de un sistema de IA que hubiera sido diseñado o implementado de modo defectuoso, no hubiera contado con una validación o prueba adecuada que condujera a errores, no contara con la documentación o instrucciones apropiadas, e incluso cuando no hubiera contado con las actualizaciones o el mantenimiento correspondiente. En consecuencia, la publicación de la Directiva (UE) 2024/2853 constituye un destacable acontecimiento jurídico que, ya de por sí, resulta merecedor de un análisis.

En consecuencia, el presente estudio persigue dar cuenta de las novedades que incorpora y de las consecuencias que se derivan de la entrada en vigor de la Directiva (UE) 2024/2853, en términos de permitir el resarcimiento de los consumidores y de otras personas físicas en el ámbito europeo, a la hora de atender a las consecuencias legales que se derivan de los daños que la Tecnología de la Información y Comunicación (TIC) y las más disruptivas como la IA, pueden generar en tanto que "producto"[20]. Y ello, por

16. *DO* L 210, de 7 de agosto de 1985.
17. ATIENZA NAVARRO, M.L., "¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)", *InDret* 2023.2, pp. 1-53, pp. 3-5.
18. RODRÍGUEZ DE LAS HERAS BALLELL, T., "The revisión of the producto liability directive: a key piece in the artificial intelligence liability puzzle", *ERA Forum,* vol. 24, 2023, pp. 247-259, p. 258; WENDEHORTS, C., "Die neue Produkthaftungsrichtlinie — ein Beispiel gelungener Mordenisierung", *GPR* 2024.4, pp. 148-157, p. 157.
19. KNETSCH, J., "Are Existing Tort Theories Ready for AI? A Continental European Perspective", en: Dimatteo, L.A. (Ed.), *The Cambridge Handbook of Artificial Intelligence*, Cambridge University Press, Cambridge (2022), pp. 99-115, p. 107.
20. No se abordará en este estudio, sin embargo, la problemática que suscita la personalidad jurídica del sistema de IA y sus consecuencias para el sector de la responsabilidad

trata de atender debidamente a los nuevos retos y riesgos que se derivan de tales tecnologías por su falta de seguridad, tal y como ya se apreciaba en el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (Texto pertinente a efectos del EEE) (Directiva riesgos)[21].

5. Eso sí, el examen de este tipo de supuestos de responsabilidad civil, además de la perspectiva armonizadora sustantiva que ha supuesto, ha de tener en cuenta igualmente su dimensión internacional. Y ello, como resultado directo de la más que previsible naturaleza transfronteriza que es susceptible de rodear a la comercialización y la utilización de los sistemas de IA; así como, y como resultado de lo expuesto, en atención al carácter transfronterizo de los daños que estos pudieran ocasionar en las personas y sus bienes. Por lo tanto, resulta importante aproximarse a los desafíos legales que supone la ordenación de la responsabilidad civil por los daños causados con mediación de los sistemas de IA y de sus resultados, en especial en tanto que eventuales productos defectuosos, no sólo desde la perspectiva sustantiva, sino también desde la óptica del Derecho Internacional privado (DIPr) —un análisis que se desarrollara, en concreto, desde la perspectiva de la determinación de la ley aplicable—, así como evaluar si el marco normativo vigente ofrece una respuesta legal adecuada a este desafío. Un examen del marco legal aplicable a tales supuestos en nuestros días, que se llevará a cabo principalmente desde la perspectiva de la UE, y al que se dedican las próximas páginas.

II. LA REGULACIÓN EUROPEA DE LA RESPONSABILIDAD CIVIL OCASIONADA POR SISTEMAS DE INTELIGENCIA ARTIFICIAL: ESTADO DE LA CUESTIÓN E IMPACTO EN LA MODERNIZACIÓN DEL RÉGIMEN DE RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS

6. Como se acaba de destacar, la Directiva (UE) 2024/2853, además de su inclusión en la estrategia europea en materia de responsabilidad civil, se inserta claramente en el contexto de la "Estrategia Digital Europea", estando

civil. Sobre esta controvertida cuestión, ATIENZA NAVARRO, M.L., *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona (2022), pp. 77-131.

21. *DO L 135 de 23 de mayo de 2023.*

así vinculada a la elaboración de las "Leyes digitales"; reflejando, de este modo, el interés manifestado por las instituciones de la UE por la regulación de los daños susceptibles de ocasionarse por los sistemas de IA[22]. Una atención por esta materia que estaría motivada, en línea de principio y entre otros objetivos, en la mejora del buen funcionamiento del mercado interior, al igual que favorecer confianza en la IA, así como orientada a ofrecer un elevado nivel de seguridad jurídica y evitar la fragmentación normativa en la UE; a la vez que, más en particular, respondería a la finalidad de favorecer el resarcimiento de los sujetos que pudieran verse perjudicados por el uso y los resultados de esta novedosa tecnología y por la posible responsabilidad civil ocasionada. Unos loables fines que, en último extremo, habría derivado en el interés en proporcionar una ordenación apropiada de este ámbito, en el marco del paquete de "Leyes de responsabilidad en materia de IA" de la UE al que se ha hecho referencia.

7. En todo caso, para entender el alcance autentico de este impulso normativo en el ámbito del Derecho de daños, hemos de ser plenamente conscientes que los esfuerzos regulatorios realizados en el ámbito de la UE se encuentran enmarcados entre dos tendencias fundamentales que condicionan al propio paquete de "Leyes digitales" —y, por ende, afectan a su vez al paquete de "Leyes de responsabilidad en materia de IA" de la UE—. En este sentido, la elaboración de la Directiva (UE) 2024/2853, de un lado, se ve afectado por el conocido como "constitucionalismo digital" europeo; mientras que, de otra parte, estaría directamente condicionado por el propósito de preservar la "soberanía digital" europea.

8. De un lado y en atención al propósito de preservar el denominado "constitucionalismo digital" europeo[23], la nueva regulación prevista para la regulación del Mercado Digital Europeo —así como, en particular, la prevista para la responsabilidad derivada de productos defectuosos—

22. En este sentido igualmente, GÓMEZ LIGÜERRE, C., "La nueva Directiva de responsabilidad por daños causados por productos defectuosos", *La Ley Unión Europea*, núm. 133, 2025, pp. 1-5, p. 2; HERBOSA MARTÍNEZ, I., "Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos". *InDret* 2024.3, pp. 52-98, pp. 60-61; RODRÍGUEZ DE LAS HERAS BALLELL, T., *op. cit.*, p. 258.

23. Sobre esta cuestión, DE GREGORIO, G.: *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge (2022), pp. 4, 21, 66 y 213; CELESTE, E.: "Digital constitutionalism. Mapping the constitutional response to digital technology's challenges", *HIIG Discussion paper series,* vol. 2, 2018, pp. 1-23, p. 17; REDEKER, D., GILL, L. y GASSER, U.: ¿"Towards digital constitutionalism? Mapping attemps to craft an Internet Bill of Rights", *The International Communication Gazette,* vol. 80, núm. 4, 2015, pp. 302-319, p. 303.

respondería al objetivo de que la UE contara con un marco normativo apropiado que, por medio de su especialización, se orientaría a garantizar la protección de los valores y de los derechos fundamentales europeos —establecidos en la Carta de los Derechos Fundamentales de la Unión Europea[24]—; al igual que perseguiría restringir las asimetrías y fomentar el equilibrio entre los operadores económicos globales y los Estados miembros —con una finalidad protectora de los intereses y derechos de las personas que residen en la UE— por medio de una regulación estricta para los operadores e intermediarios que actuasen en el UE en el nuevo contexto tecnológico.

En esta línea, por un lado, cabría mencionar la relevante "Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital" de 2022[25] y, en particular, lo previsto en sus Capítulos III en el ámbito de la "Libertad de elección" —al referirse a la necesidad de velar por un entorno digital seguro y protegido— y el V relativo a la "Seguridad, protección y empoderamiento" —cuando se refiere a la necesidad de garantizar un entorno digital protegido y seguro—. Además, esta finalidad se apreciaría igualmente, en particular y ya en el contexto de la Directiva (UE) 2024/2853, en el objetivo que se marca "de crear un auténtico mercado interior con un elevado y uniforme de protección de los consumidores"[26].

9. Por su parte y al respecto del objetivo de preservar la "soberanía digital" europea, no hemos de perder de vista, para empezar, que los avances legislativos en la materia examinada —como todos aquellos que se encuentran relacionados con las nuevas tecnologías— poseen un carácter altamente estratégico; en un marco global competitivo donde debe tutelarse el modelo digital, los valores y los principios que promuevan la innovación y la autonomía tecnológica de la UE, así como fomentar su liderazgo en este ámbito[27]. Tal y como se ha subrayado recientemente en la Comunicación y Plan de Acción de la Comisión "Continente de IA"[28]. Además, en relación con

24. *DO* L 83, de 30 de marzo de 2010.
25. COM (2022) 28 final. Téngase en cuenta, RIVAS VELASCO, M.J.: "Principios éticos de las IAs e impacto en derechos fundamentales", *Diario La Ley*, núm. 93, Sección Ciberderecho, 14 de marzo de 2025, pp. 1-18.
26. Considerando 8.
27. FERNÁNDEZ ROZAS, J.C., "La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo", *La Ley Unión Europea,* núm. 124, 2024, pp. 1-69, pp. 2-5.
28. COM (2025) 165 final, p. 29. Al respecto, CZERNIAWSKI, M.: "Towards the effective extraterritorial enforcement of the IA Act", en HOEPMAN, J.H., JENSEN, M., PORCEDDA, M.G., SCHIFFNER, S., ZIEGLER, S., (Eds.), *Privacy Symposium 2024 — Data Protection Law International Convergence and Compliance with Innovative Technologies*

ello, ha de tener en consideración los objetivos que orientan al legislador europeo al elaborar la Directiva (UE) 2024/2853, tanto por el fomento de la implantación de tales tecnologías, como por no obstaculizar la innovación en esta materia[29].

Un interés, este último, que además se encontraría directamente vinculado a la finalidad de hacer frente a las vulnerabilidades en materia de "Ciberseguridad" que amenazan a la UE y a los ciudadanos, y a las que se refieren: las Comunicaciones de 2020 "Sobre la Estrategia de la UE para una Unión de la Seguridad"[30] y "La Estrategia de Ciberseguridad de la UE para la Década Digital"[31]; al igual que, ya en 2022, es destacada en la publicación de la "Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa"[32]. De este modo y descendiendo a la materia examinada, se advierte como la preocupación que muestra el legislador europeo por las cuestiones en materia de "Ciberseguridad" se recoge en la Directiva (UE) 2024/2853 en diversas ocasiones, mencionando los requisitos que los operadores económicos deben cumplir para evitar los riesgos en este ámbito[33].

1. LOS ESFUERZOS DEL LEGISLADOR EUROPEO POR ESTABLECER UN MARCO REGULATORIO EN RELACIÓN CON LA RESPONSABILIDAD CIVIL DERIVADA DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

10. Ahora bien, en atención a los mencionados objetivos y el lugar tan destacado que ocupa el establecimiento de un régimen de responsabilidad civil adaptado a la era de la IA, el camino recorrido por las instituciones europeas para poder contar con un marco jurídico adaptado a los avances tecnológicos no ha sido sencillo. En este sentido, se observa como el establecimiento de un conjunto de "Leyes de responsabilidad en materia de IA" europeas no está resultando sencillo, siendo numerosos los documentos que se han ido publicando por parte de las instituciones de la UE y en este ámbito durante los últimos años.

(DPLICIT), Springer, Frankfurt a.M. (2025), pp. 1-20, p. 11; ROBLES CARRILLO, M.: "La articulación de la soberanía digital en el marco de la Unión Europea", *Revista de Derecho Comunitario Europeo,* núm. 75, 2023, pp. 133-171, pp. 147 y 150-153.

29. Considerandos 3 y 14.
30. COM (2020) 605 final, pp. 15 y 30.
31. JOIN (2020) 18 final, pp. 6, 22 y 24.
32. COM (2022) 61 final, pp. 6 y 9.
33. Así, los Considerandos 32, 34, 52, 55, como en el art. 7.2, f) a la hora de valorar el carácter defectuoso de un producto.

11. Así, sobre este esfuerzo regulatorio llevado a cabo en el ámbito de la responsabilidad civil derivado del uso y de los resultados de los sistemas de IA, resulta de utilidad mencionar su evolución cronológica, para entender el alcance del esfuerzo regulador llevado a cabo en este ámbito por parte del legislador europeo.

a) Así las cosas, por lo que hace a su inicio, cabe destacar como el mismo partió de la publicación en 2016 del Estudio "European Civil Law Rules in Robotics"[34]. Al cual siguió en 2017 la Resolución del Parlamento Europeo, con recomendaciones destinadas a la Comisión, "sobre normas de Derecho civil sobre robótica"[35]. Sin embargo, fue en la Comunicación de la Comisión de 2018 cuando se destacó la necesidad de abordar la materia de la responsabilidad civil en materia de IA —tanto con carácter general, como en relación con los productos defectuosos—[36]. Por su parte, sería en 2019 cuando viera la luz la Comunicación "Generar confianza en la Inteligencia Artificial centrada en el ser humano" —donde se insistiría en la necesidad de ordenar el ámbito de la responsabilidad civil—[37].

b) Aunque sería en 2020 cuando se daría un paso decisivo en este ámbito por pate de la Comisión, al menos en un inicio, comenzando por la publicación del "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica"[38], del "Libro Blanco sobre la Inteligencia Artificial — un enfoque europeo orientado a la excelencia y la confianza"[39] y de la Comunicación "Configurar el futuro digital de Europa"[40]. Un impulso al que siguió, ese mismo año y tras la publicación de la Resolución del Parlamento Europeo "sobre la inteligencia artificial en la era digital" —donde se hizo un a especial incidencia en los aspectos relativos a la responsabilidad civil y señaladamente a la derivada de productos defectuosos—[41], la presentación de un Informe con recomendaciones para la Comisión que, elaborado por el Parlamento

34. El cual fue elaborado, a instancias del Parlamento Europeo, por la Profesora Nathalie Nevejans, y que se encuentra disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf.
35. P8_TA (2017) 0051.
36. COM (2018) 237 final, p. 19.
37. COM (2019) 168 final, pp. 10-11.
38. COM (2020) 64 final.
39. COM (2020) 65 final, p. 31.
40. COM (2020) 67 final.
41. P9_TA (2022) 0140. En especial, en sus apartados 130 a 146. Una Resolución que sucede a las Resoluciones sobre los "Procesos automatizados de toma de decisiones: garantizar la protección de los consumidores" y "Sobre una nueva estrategia industrial para Europa" (P9_TA (2020) 0032 y P9_TA (2020) 0321, respectivamente).

Europeo, se refirió al establecimiento de "un régimen de responsabilidad civil en materia de inteligencia artificial"[42]. En relación con ello, el Consejo dio luz verde a todas estas iniciativas en el contexto de sus "Conclusiones sobre el diseño del futuro digital de Europa" de 2020[43].

c) Con posterioridad, ya en el año 2021, tras recordar la relevancia de adaptar el marco relativo a la responsabilidad civil e igualmente revisar la normativa sobre productos defectuosos en el ámbito de la IA, así como la necesidad de mantener la coherencia y la complementariedad entre las distintas iniciativas de la UE para la IA, en la Comunicación "Fomentar un planteamiento europeo en materia de Inteligencia Artificial"[44], se presentó la Comunicación "Fomentar un planteamiento europeo en materia de Inteligencia Artificial"[45], viendo con posterioridad la luz un completo análisis comparado promovido desde la Comisión titulado "Comparative Law Study on Civil Liability for Artificial Intelligence"[46]; siendo de ese mismo año el informe elaborado por la DG Connect de la propia Comisión de ese mismo año "Study to Support the Commission's Impact Assessment on Liability for Artificial Intelligence"[47].

d) No obstante, 2022 resultó ser un año singularmente significativo, al ser cuando la Comisión publicó sendas Propuestas de Directiva, tanto "relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)"[48], como "sobre responsabilidad por los daños causados por productos defectuosos"[49]. Aunque se tuvo que esperar hasta el 2024 para la publicación del estudio presentado por el Parlamento Europeo, donde se incluyó una Evaluación de impacto complementaria y una "Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence".

---

42. A9-0178/2020.
43. *DO* C 202, de 16 de junio de 2020, p. 23.
44. COM (2021) 205 final, p. 3.
45. COM (2021) 205 final.
46. El cual fue elaborado por los Profesores Ernst Karner, Bernhard A. Koch y Mark A. Geistfeld, y se encuentra disponible en: https://op. europa.eu/en/publication-detail/-/publication/8a32ccc3-0f83-11ec-9151-01aa75ed71a1/language-en.
47. Accesible en: https://op. europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en.
48. COM (2022) 496 final.
49. En COM (2022) 495 final y COM (2022) 496 final. *Vid.* MARTÍN CASALS, M., "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *InDret* 2023.3, pp. 55-100, pp. 71-93; REYES LOPEZ, M.J., "Inteligencia artificial y relaciones de consumo", en RAMOS FERNÁNDEZ, F. (Coord,), *Ciencia de datos y perspectivas de la inteligencia artificial,* Tirant lo Blanch, Valencia (2024), pp. 104-143, pp. 120-130.

12. En todo caso, el balance regulatorio alcanzado en este ámbito hasta la fecha deja un sabor ciertamente agridulce. Toda vez que la consecuencia más palpable de este esfuerzo codificado, hasta la fecha, lo constituye únicamente la publicación de la Directiva (UE) 2024/2853; dejándose *sine die* la continuación de los trabajos en materia de responsabilidad civil extracontractual derivada de IA. Así las cosas, poco se puede esperar en el avance de la "Propuesta de Directiva sobre responsabilidad en materia de IA" de 2022, debido a su reciente exclusión de los futuro trabajos de la Comisión, al no resultar previsible que se alcance un acuerdo sobre la misma[50]. Todo lo cual redunda en la actual falta de seguridad jurídica en este ámbito y, por tanto, afectando negativamente en el empleo e inversión en el ámbito de la IA[51].

Consecuentemente, la Directiva (UE) 2024/2853 se erige en la actualidad como el único instrumento normativo elaborado por el legislador europeo que aborda cuestiones de responsabilidad civil con incidencia en el ámbito de la IA. Nos situamos, por tanto, ante un proceso de armonización de naturaleza sustantiva inacabado y fragmentario, que pone en tela de juicio el cumplimento de los objetivos que inspiran al legislador europeo en este sector que, como se ha expuesto, se dirige a favorecer el buen funcionamiento del mercado interior, así como de ofrecer un nivel adecuado de seguridad jurídica e incrementar la confianza de los ciudadanos en la IA.

13. En todo caso, igualmente han de ser tenidos en cuenta en este sector, y con incidencia directa en el ámbito de la responsabilidad derivadas de productos defectuosos, tanto el Reglamento 2023/988 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo[52], como el Reglamento 2023/1230 relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo[53].

Todo ello sin olvidar que, aun cuando deje intacta la normativa reguladora de la responsabilidad civil y únicamente pretenda establecer obligaciones de carácter administrativo a los operadores económicos en materia

50. Tal y como se aprecia en la Comunicación de la Comisión "Programa de trabajo de la Comisión para 2025. Avanzar juntos: Una Unión más audaz, más sencilla y más rápida", en su Anexo IV, p. 26.
51. ATIENZA NAVARRO, M.L., "¿Una nueva responsabilidad…", *op. cit.*, p. 49.
52. *DO* L 135, de 23 de mayo de 2023.
53. *DO* L 165, de 29 de junio de 2023.

de IA[54], pero en atención a su carácter horizontal y a las exigencias que impone a estos sujetos —en cuanto que norma de derecho público regulatorio, preocupadas por la seguridad de los sistemas de IA—, sus preceptos igualmente pueden ser considerados como base para una reclamación civil por el incumplimiento de las obligaciones de seguridad que establece el Reglamento de IA[55].

2. LA DIRECTIVA (UE) 2024/2853 SOBRE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS Y SU IMPACTO EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL

14. Como se acaba de destacar, desde que las instituciones de la UE tomaron conciencia de la relevancia que poseía adaptar la normativa relativa a la responsabilidad civil al ámbito de la IA, se decidió actuar desde una doble perspectiva. Así, por un lado, se habría propuesto generar un marco normativo de carácter sustantivo que ofreciera una armonización de las reglas estatales de naturaleza material reguladora de las consecuencias civiles derivadas de los daños ocasionados como resultado de los sistemas de IA. Una vía que, como se acaba de constatar, se encuentra paralizada de momento, tras haber sido apartada en el Plan de Acción de la Comisión para 2025.

Junto a ello, la otra alternativa se habría orientado a adaptar y modernizar el marco legal en materia de productos defectuosos a las exigencias que se derivan del nuevo contexto tecnológico, así como por la introducción de la IA[56]. Una actuación regulatoria más exitosa y que habría conducido a la aprobación de la Directiva (UE) 2024/2853, a la que nos referiremos seguidamente. En este sentido y como se puso de manifiesto en el anterior apartado, la posibilidad de modificar la Directiva 85/374/CEE para adaptarlo al nuevo contexto de la IA se encontraba ya presente de forma reiterada en todos los documentos que, desde 2016, se han ido confeccionado por las instituciones de la UE con relación a la ordenación de la IA. Junto a ello, se trataba de una

54. Considerando 9.

55. HENCKEL, K., "Issues of conflicting laws — a closer look at the EU's approach to artificial intelligence", *NIPR*, 2023-12, pp. 199-226, p. 205; RUBI PUIG, A., "Una lectura del Reglamento de Inteligencia Artificial desde del derecho privado", *InDret* 2024.4, pp. i-viii, pp. ii-iv.

56. *Vid*. CAPPIELLO, B., *AI-systems and non-contractual liability. A european private internatinla law analysis*, Giappichelli, Turín (2022), pp. 72-75; LAFUENTE SÁNCHEZ, R., *Inteligencia artificial y vehículos autónomos: responsabilidad civil extracontractual internacional*, Aranzadi, Pamplona (2024), pp. 115-130.

materia sobre la que había un cierto consenso sobre la necesidad de llevar a cambio una revisión de la normativa existente.

15. En esta línea, aunque con una naturaleza de *Soft Law*, destaca igualmente el interés que esta cuestión despertó en el seno del *European Law Institute* (ELI), así como su significativa aportación al respecto de su estudio y de su posterior desarrollo normativo. Una preocupación que se puso de manifiesto ya con la elaboración de los "Guiding Principles for Updating the Product Liability Directive for the Digital Age" de 2021[57]. Unos principios a los que siguieron, además de su respuesta a la "European Commission's Public Consultation on Civil Liability Adapting Liability Rules to the Digital Age and Artificial Intelligence" de 2022[58], la elaboración del "ELI Draft of a Revised Product Liability Directive" del mismo año y por lo que respecta de forma particular a la materia analizada[59]. A este respecto cabe destacar, como resultado de tales estudios, tanto el significativo valor de las aportaciones realizadas por el ELI, así como la importancia de esta contribución académica, por lo que hace a la revisión y modernización de la Directiva 85/374/CEE.

16. De esta forma y teniendo en consideración la base jurídica que ofrecía el art. 114 del TFUE, la finalidad principal que orientó al legislador europeo en este ámbito no podía ser otras que la puesta al día de la Directiva 85/374/CEE, al no encontrase adaptada a la nueva realidad tecnológica, que sencillamente no contemplaba debido al momento en que fue elaborada. Por lo que resultaba imperativo su sustitución por un nuevo instrumento con el que se actualizara la respuesta normativa a este tipo de daños[60]. Y ello, en vistas tanto a fomentar la implantación y la aceptación de las nuevas TICs —incluido el uso de los sistemas de IA— de modo que los sujetos perjudicados por los resultados de su uso pudieran contar con un mismo nivel de protección con independencia de la tecnología de que se tratase, ofreciendo a las empresas un elevado nivel de seguridad jurídica y de unas condiciones de competencia equitativas[61]; así como para garantizar la coherencia y la uniformidad al respecto de la normativa de la UE sobre seguridad de los productos y la vigilancia del mercado —tanto nacional, como europeo—,

57. Preparado por el Profesor Christian Twigg-Flesner, dentro del *ELI Innovation Paper Series*. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Guiding_Principles_for_Updating_the_PLD_for_the_Digital_Age.pdf
58. En: https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf
59. En: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf
60. Considerando 5.
61. Considerando 3.

además de clarificar ciertos conceptos básicos a partir de los que fomentar la coherencia y la seguridad jurídica, al igual que unas condiciones de competencia equitativas en el mercado interior[62].

Con tal finalidad en mente, el art. 1 de la Directiva (UE) 2024/2853 dispone que, mientras su objeto lo constituye establecer un marco normativo armonizado relativo a la "*la responsabilidad de los operadores económicos por los daños sufridos por personas físicas causados por productos defectuosos y sobre la indemnización por esos daños*" (párrafo I); su objetivo se centra en favorecer "*el correcto funcionamiento del mercado interior, garantizando al mismo tiempo un elevado nivel de protección de los consumidores y otras personas físicas*" (párrafo II). Para ello, como ya sucedía con la Directiva de 1985 (art. 12), la nueva regulación establece una regulación armonizada de naturaleza sustantiva y de carácter imperativo, como dispone actualmente su art. 15. A su vez y como subraya el articulo 3 al establecer el nivel de armonización que persigue la Directiva —un extremo novedoso de cara al régimen precedente—, impide a los Estados miembros que mantengan o introduzcan, en su Derecho nacional, disposiciones que se aparten de las establecidas en la Directiva y por medio de las que se ofrezca un nivel diferente de protección a las personas perjudicadas[63].

17. Una cuestión que posee una singular relevancia y que va a afectar al tratamiento conflictual de los supuestos de responsabilidad derivada de productos con un carácter internacional, se refiere a la concreción del ámbito de aplicación de la nueva Directiva se recoge principalmente su Capítulo I, donde se sitúan sus disposiciones generales. Así, por un lado y desde una perspectiva temporal, en su numeral 1.º se dispone que la aplicación de esta se contempla para los productos introducidos en el mercado o puestos en servicio después del 9 de diciembre de 2026. A su vez, desde un punto de vista territorial, el art. 24 comprende como destinatarios de la Directiva (UE) 2024/2853 a los Estados miembros de la UE —aunque sin hacer mención alguna al respecto de la concreción del ámbito de aplicación territorial de las soluciones que contiene[64]—.

18. Junto a ello y por lo que respecta al ámbito de aplicación material, junto a lo expuesto en el art. 1 al establecer su objeto, hay que tener en consideración lo consignado en los apartados 2 a 4 del art. 2, al igual que lo previsto en el art. 4 donde se contienen una serie de definiciones de gran relevancia.

62. Considerando 4.
63. Considerando 8. *Vid*. VAN DAM, C., *European Tort Law*, Oxford University Press, Oxford (2006), p. 24.
64. FRANCQ, S., *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruylant, Bruselas (2005), p. 349.

a) Así las cosas, de un lado, en los mencionados numerales del art. 2 se contempla la dimensión negativa del ámbito de juego sustantivo de la nueva Directiva, al establecer que la misma no se aplicará a: "*los programas informáticos libres y de código abierto que se desarrollen o suministren fuera del contexto de una actividad comercial*" (apartado 2) —a fin de no poner obstáculos a la investigación y la innovación—[65]; "*los daños derivados de accidentes nucleares*" —tal y como ya se preveía en el art. 14 de la Directiva 85/374/CEE[66]— (apartado 3); así como tampoco va a afectar a otros ámbitos que ya cuentan con un régimen propio de responsabilidad, tal y como sucede con la normativa de la UE sobre la protección de datos personales[67], la propia de los Estados miembros en materia de responsabilidad contractual o extracontractual "*por motivos distintos del carácter defectuoso de un producto*" relacionadas con la Directiva, con la inclusión de aquellas normas estatales por medio de las que se aplica el Derecho UE, o aquellos derechos que el sujeto perjudicado pudiera tener de conformidad a un régimen especial de responsabilidad que se encontrara vigente a 30 de julio de 1985 (apartado 4).

b) Por otra parte, el art. 4 contempla una serie de definiciones autónomas de necesaria interpretación uniforme por parte del TJUE, que cuentan con un gran valor armonizador, entre las que destaca la propia noción de "producto". Un concepto que, sin lugar a duda, posee una gran relevancia y se concibe en su numeral 1.º como "*cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; incluye la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos*". De tal manera que la nueva Directiva implicaría, no sólo una adaptación al nuevo medio tecnológico, sino una ampliación del estricto concepto que mantenía el art. 2 de la Directiva 85/374/CEE, que se veía limitada a los productos físicos y, por tanto, a los bienes muebles[68].

---

65. Considerados 14 y 15. Sobre esta exclusión, GÓMEZ LIGÜERRE, C., *op. cit.*, pp. 6-7.
66. Considerando 7. Un ámbito que cuenta con un marco regulatorio de naturaleza convencional, donde destaca el Convenio de París sobre responsabilidad civil en materia nuclear, de 1960 (*BOE* núm. 28, de 2 febrero de 1967).
67. En particular el Reglamento (UE) 2016/679 —ya citado—, así como el Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento 2018/1724 (*DO* L 152, de 3 junio de 2022) o el Reglamento (UE) 2023/2854, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (*DO* L 2023/2854, de 22 de diciembre de 2023).
68. En este sentido, ATIENZA NAVARRO, M.L., "¿Una nueva responsabilidad…", *op. cit.*, pp. 7-12.

19. En relación con la delimitación de "producto", no cabe duda de que el legislador europeo debía actualizar y ampliar el concepto empleado en la Directiva de 1985, con el objeto de adaptarlo a los daños generados por el avance tecnológico y los sistemas de IA[69]. Tal es el objetivo perseguido por la nueva regulación europea. Sobre esta cuestión, podría llegar a poner en duda si efectivamente la Directiva (UE) 2024/2853 cubriría los sistemas de IA, debido a que de una lectura conjunta y estricta de sus arts. 1, 2 y 4, no se aprecia su inclusión con total claridad, al no realizarse mención directa a la IA. Sin embargo, en nuestra opinión y a pesar de esa constatación literal, no puede ponerse en tela de juicio su plena aplicación, no sólo en consideración del contexto regulatorio en el que se enmarca, sino particularmente a un gran número de supuestos relacionados con este tipo de tecnologías disruptivas y, por tanto, la inclusión de distintos sistemas de IA en el concepto de "producto" que utiliza el art. 4.1 de la Directiva[70].

a) En este sentido y con carácter preliminar y por lo que hace al contexto regulatorio en el que se enmarca, cabe recordar como la nueva Directiva sirve a un claro interés del legislador europeo en contar con un marco normativo adaptado a los desafíos legales que suponen los sistemas de IA. De este modo, ya se ha puesto de manifiesto como, en el largo proceso legislativo que precedió a la publicación de Directiva (UE) 2024/2853, se puso constantemente el acento en la importancia de modernizar el marco armonizado existente a la nueva realidad tecnológica y la implantación de la IA; existiendo una estrecha relación y objetivo compartido de enfrentar los retos legales que suponía la IA, entre la nueva Directiva y la, recientemente abandonada, Propuestas de Directiva sobre responsabilidad en materia de IA[71].

En esta línea, ha de tenerse en cuenta en particular, como ya la Propuesta de Directiva presentada en 2022 llevó a cabo numerosas menciones a la IA, destacando como uno de los objetivos regulatorios la adaptación del marco vigente —incluida la materia de la responsabilidad derivada de productos defectuosos— a esta nuestra realidad tecnológica. A modo de ejemplo, no sólo se mencionó esta tecnología al mencionar las deficiencias que presentaba la Directiva 85/374/CEE en relación con la carga de la prueba, demostrar que el producto era defectuoso y que la IA había causado los daños que se habían sufrido[72], sino también se hizo referencia a la estrecha relación que

69. CAPPIELLO, B., *op. cit.*, p. 144.
70. *Vid*. HERBOSA MARTÍNEZ, I., *op. cit.*, pp. 93-94; MÜLLER-BERG, M.F., "Die Auswirkingen der neuen Produkthaftungsrichtlinie auf die internationale Produkthaftung", *IPrax* 2025. 3, 221-230, p. 223.
71. WENDEHORTS, C., *op. cit.*, pp. 155-156.
72. COM (2022) 495 final, p. 1.

la materia de la responsabilidad por productos —al igual que la vinculada a su seguridad— mantenía con el Reglamento de IA[73].

b) Junto a ello, y por lo que hace a la evidente incorporación de ciertos sistemas de IA en la definición de "producto" que se ofrece en la Directiva (UE) 2024/2853, igualmente se ha de llegar a la misma interpretación —además de por el contexto de elaboración y el propio *iter* legislativo que ya ha sido mencionado— a partir de una interpretación sistemática y teleológica del nuevo instrumento europeo; teniendo por tanto en consideración su coherencia con los objetivos perseguidos por el legislador europeo al llevar a cabo esta modernización normativa.

Así las cosas, para empezar, se debe alcanzar esta conclusión inclusiva toda vez que en el Considerando 3, al referirse a la finalidad que se persigue con la Directiva, se hace mención particular de la voluntad del legislador europeo de adaptar el anterior marco normativo en la materia a los avances relacionados con las TICs "incluida la inteligencia artificial (IA)", con el fin de la implantación y aceptación de estas tecnologías novedosas. Una referencia a las nuevas tecnologías y, en particular, a la posible consideración de los programas informáticos como productos defectuosos en el Considerando 6.

En el mismo sentido, si se toma en consideración lo previsto en su Considerando 13, al referirse a los productos en el contexto de la era digital, se menciona en el contexto de su juego al respecto de los programas informáticos, a "los sistemas de IA", destacando su relevancia en el ámbito de la seguridad de los productos. Por último, igualmente se hace referencia directa a la IA en los Considerandos 40, cuando aborda la cuestión de la modificación sustancial que podría sufrir un producto por medio de —entre otros— "el aprendizaje continuo de un sistema de IA"; y en el 48, al mencionar los problemas que suscita la determinación del nexo causal entre el daño y el defecto, pone como ejemplo un supuesto de una demanda relacionada con los sistemas de IA.

20. Por todo lo expuesto, entendemos que resulta difícil negar que la nueva Directiva en materia de productos defectuosos resulta de aplicación al ámbito de la IA. Como resultado de esta toma de postura, una vez determinado su ámbito de aplicación y se ha verificado la plena aplicación de Directiva (UE) 2024/2853 al contexto de la IA, debe hacerse mención a sus elementos principales. Un repaso de su articulado que, sin ánimo de exhaustividad —al no constituir el objeto último de este estudio—, evidencia los relevantes cambios que incorpora frente al modelo establecido en 1985.

73. *Ibid.*, p. 4.

21. Para empezar, su Capítulo II incorpora las "Disposiciones específicas sobre la responsabilidad por productos defectuosos" (arts. 5 a 11). En este sentido, en su art. 5 se aborda el derecho a indemnización que debe garantizarse a toda persona física que hubiera sufrido daños por motivo de un producto defectuoso, así como las personas legitimadas para presentar las reclamaciones de indemnización oportunas —sucesor, subrogado o en nombre de una o varias personas perjudicadas—; mientras que el art. 6 hace mención a los daños incluidos los morales que se contemplen en el Derecho nacional —que dan derecho a solicitar tal indemnización— haciendo referencia únicamente a la muerte o lesiones corporales, a los bienes o su destrucción, sin cubrir el propio producto defectuoso, o por un componente defectuoso o interconectado a él por el fabricante o bajo su control, o los bienes utilizados con fines profesionales; sin afectar a las indemnizaciones contempladas en regímenes de responsabilidad distintos al de la Directiva. Como novedad, cabe destacar la inclusión de activos inmateriales como los datos por la destrucción o corrupción de datos que no tuvieran un uso profesional, que no se encontraba presente en la Directiva 85/374/CEE[74].

Por su parte, y de gran relevancia en esta materia, en el art. 7 se establece las circunstancias que se habrán de tomar en consideración para determinar el carácter defectuoso del producto, siempre que no ofrezca seguridad que se tenga derecho a esperar exigido en la normativa UE o la propia del Estado miembro[75]; excluyendo los supuestos en los que se hubiera introducido posteriormente en el mercado un producto mejor —o sus actualizaciones—. De tal forma que por medio de este se amplía el concepto del carácter defec-

74. Considerando 20.

75. Considerado 30. Así, el art. 7.2 contempla entre tales circunstancias: "*a) la presentación y las características del producto, incluidos su etiquetado, diseño, características técnicas, composición y envase, y las instrucciones de montaje, instalación, uso y mantenimiento; b) el uso razonablemente previsible del producto; c) el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio; d) el efecto razonablemente previsible en el producto de otros productos de los que se pueda esperar que se utilicen junto con el producto, también mediante interconexión; e) el momento en que el producto fue introducido en el mercado o puesto en servicio o, si el fabricante conserva el control sobre el producto después de ese momento, el momento en que el producto dejó de estar bajo el control del fabricante; f) los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad pertinentes para la seguridad; g) cualquier retirada del producto o cualquier intervención pertinente relacionada con la seguridad de los productos por parte de una autoridad competente o de un operador económico contemplado en el art. 8; h) las necesidades específicas del grupo de usuarios finales a los que se destina el producto; i) en el caso de un producto cuya finalidad sea precisamente evitar daños, el eventual incumplimiento de dicha finalidad por parte del producto*".

tuosos que mantenía el art. 6 de la Directiva 85/374/CEE, centrado en la seguridad que podía legítimamente esperar del mismo.

Junto a ello, es el art. 8 donde se contempla quienes van a ser los operadores económicos que eventualmente podrían ser estimados como responsables de los daños ocasionados por los productos defectuosos, poniéndose el acento como es tradicional en el propio fabricante del producto o de un componente defectuoso del mismo —integrado o interconectado y que fuera el causante del defecto, sin afectar a la responsabilidad del fabricante—[76]. Aunque este precepto incluye, a tales efectos e implicando una ampliación objetiva y subjetiva en relación con la más limitada previsión contenida en el art. 3 de la Directiva 85/374/CEE, otras situaciones como serían los casos en que tales sujetos se encontraran establecidos fuera de la UE, los comercializadores, e incluso los distribuidores si no se identificase al operador en cuestión, así como situaciones propias del ámbito digital como los prestadores de servicios digitales y los proveedores de plataformas en línea por los productos defectuosos que se pudieran vender a través de las mismas[77].

Asimismo, en otro orden de ideas y subrayando el carácter de responsabilidad objetiva que establece la Directiva, incorpora disposiciones específicas en materia de prueba. Un extremo de gran complejidad en el ámbito de la IA y de gran importancia que, en los supuestos internacionales y por encontrarse los elementos probatorios el extranjero, puede encarecer e incluso llegar a malograr la reclamación de la persona perjudicada[78]. Al respecto, el art. 9 consagra *ex novo* la exigencia de que los Estados miembros garanticen mecanismos para que las partes exhiban —de modo accesible y comprensible— las pruebas oportunas de la que dispongan —sin afectar a la posibilidad de su exhibición preliminar, donde se exija—, siempre que resulte necesario y proporcionado, en consideración de los intereses legítimos de las partes —como sería la tutela de la infamación confidencial y

76. Considerando 18. El art. 2.10 define "fabricante" como "*toda persona física o jurídica que: a) desarrolla, fabrica o produce un producto; b) tiene un producto diseñado o fabricado, o que, al poner su nombre, marca u otros elementos distintivos en dicho producto, se presenta como su fabricante, o c) desarrolla, fabrica o produce un producto para su propio uso;*".

77. Considerando 38. ATIENZA NAVARRO, M.L., "¿Una nueva responsabilidad…", *op. cit.*, pp. 21-27; MARTÍN CASALS, M., *op. cit.*, pp. 82-83; MÜLLER-BERG, M.F., *op. cit.*, pp. 229-230. La jurisprudencia del TJUE ya había ido contemplando esta ampliación, como se aprecia en las SSTJUE, de 21 de diciembre de 2011, Asunto C-495/10, *Dutrueux and Caisse primaire d'assurance maladie du Jura* (ECLI:EU:C:2011:869); y de 19 de diciembre de 2024, Asunto C-157/23, *Ford Italia* (ECLI:EU:C:2024:1045).

78. MORGAN, P., *"Tort Law and AI: Vicarious Liability"*, en LIM, E. y MORGAN, P. (Eds.), *The Cambridge Handbook of Private Law and Artificial Intelligence*, Cambrigde University Press, Cambridge (2024), pp. 135-171, p. 149.

secretos comerciales[79], con el fin de preservar tal confidencialidad—[80]. En relación con ello, el art. 10 aborda la relevante cuestión de la carga de la prueba del carácter defectuoso del producto y el nexo causal entre el mismo y el daño que va a recaer sobre el demandante, aunque se establecen una serie de presunciones que jugarán a favor de las persona perjudicada —sobre todo cuando se refiera a complejas cuestiones tecnológicas— y que podrá refutar el demandado —implicando una cierta reversión de la carga de la prueba, incorporando una novedad frente a lo previsto en el art. 4 Directiva 85/374/CEE—[81].

Por último, el Capítulo finaliza con el art. 11 establece una serie de supuestos de exención, a partir de los que los operadores económicos —a los que se refiere el art. 8— puedan demostrar su falta de responsabilidad[82]; aunque esto no sería posible si, bajo su control, se tratara de un servicio conexo, programas informáticos —con inclusión de las actualizaciones o mejoras—, falta de actualizaciones o mejoras de los programas informáticos que fueran necesarias para mantener la seguridad, o una modificación sustancial del producto[83]. Por lo tanto, se aprecia como incorpora nuevas obligaciones de transparencia y de trazabilidad para el sujeto responsable, frente a las previsiones contenidas en el art. 5 de la Directiva 85/374/CEE.

---

79. Tal y como es definido en el art. 2.1 de la Directiva (UE) 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (*DO* L 157, de 15 de junio de 2016). *Vid.* Considerando 45.
80. Considerandos 42 a 44. GÓMEZ LIGÜERRE, C., *op. cit.*, p. 10.
81. Considerando 48. ATIENZA NAVARRO, M.L., "¿Una nueva responsabilidad…", *op. cit.*, pp. 32-37.
82. En particular, el apartado 1 se refiere a: "*a) en el caso de un fabricante o importador, que no ha introducido el producto en el mercado ni lo ha puesto en servicio; b) en el caso de un distribuidor, que no ha comercializado el producto; c) que es probable que el carácter defectuoso que haya causado el daño no existiera en el momento en que el producto fue introducido en el mercado, puesto en servicio o, en el caso de un distribuidor, comercializado, o que ese carácter defectuoso se originase después de ese momento; d) que el carácter defectuoso que haya causado el daño se debe a que el producto cumple requisitos legales; e) que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso; f) en el caso de un fabricante de un componente defectuoso, a que se refiere el art. 8, apartado 1, párrafo primero, letra b), que el carácter defectuoso del producto en el que se ha incorporado dicho componente sea imputable al diseño de ese producto o a las instrucciones dadas por el fabricante de tal producto al fabricante de dicho componente; g) en el caso de una persona que modifica un producto según lo dispuesto en el art. 8, apartado 2, que el carácter defectuoso que haya causado el daño esté relacionado con una parte del producto no afectada por la modificación*".
83. Cuya definición se sitúa en el art. 2.18 de la Directiva.

22. Continuando con esta somera exposición del contenido de la Directiva (UE) 2024/2853, corresponde hacer referencia a su Capítulo III, donde se incorporan las "Disposiciones generales en materia de responsabilidad" (arts. 12 a 17). Así las cosas, el Capítulo comienza con el art. 12, donde se incorpora el reconocimiento de que se responda solidariamente en supuestos de responsabilidad de múltiples operadores económicos, sin que se contemple el derecho de repetición al fabricante que incorpore un componente de programa informático en un producto —se entiende que incluida un sistema de IA—, frente al fabricante de este componente que resulte defectuoso[84]. Por su parte, en art. 13 contempla diversas cuestiones relativas a la reducción de la responsabilidad, tanto para garantizar que no se produzca por tratarse de un producto defectuoso y por una acción u omisión de un tercero, contemplando tal reducción cuando se presente tal defecto y fuera por culpa de la persona perjudicada u otra que depende de ésta.

Asimismo, el art. 14 incorpora *ex novo* el derecho de repetición de un operador económico frente otros —especialmente relevante para el sector de los programas informáticos—, en atención a lo previsto en el art. 8 y en el Derecho nacional[85]. Al igual que el art. 15 establece la garantía de que no se pueda producir la exclusión o limitación de la responsabilidad en estos casos, ya sea por una disposición contractual o por lo previsto en el Derecho nacional. Por último, los plazos armonizados de prescripción y de caducidad se recogen respectivamente en los arts. 16 y 17.

23. La Directiva (UE) 2024/2853 finaliza con un Capítulo IV que recoge un conjunto de "Disposiciones finales" (arts. 18 a 24). Para comenzar, el art. 18 reconoce la tradicional excepción a la exoneración de las obligaciones establecidas en el art. 11 basada en los "riesgos de desarrollo"[86], por medio de una regulación singularmente detallada. Sobre el mismo destaca novedad que implica la remisión que realiza al art. 11.1, e) la referencia al estado de los conocimientos científicos o técnicos, como podrían ser las relacionadas con los sistemas de IA[87].

A su vez, este Capítulo incluye por vez primera una serie de obligaciones relativas a la transparencia de las decisiones judiciales que se dicten en este

84. Considerado 53. GÓMEZ LIGÜERRE, C., *op. cit.*, p. 13.
85. Considerando 54.
86. Contemplando, en su apartado 1.º, que los operadores económicos seguirán siendo considerados como responsables "*aunque demuestren que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado o puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso*".
87. Considerando 59. ATIENZA NAVARRO, M.L., *op. cit.*, pp. 41-43.

ámbito (art. 19), su evaluación (art. 20)[88], así como otros extremos novedosos relacionados con las disposiciones derogatorias y transitorias (art. 21), la transposición de la Directiva que se prevé para el 9 de diciembre de 2026 "como tarde" (art. 22), así como otras —a las que ya se ha hecho referencia— como su entrada en vigor el 8 de diciembre de 2024 (art. 23) y la mención de los Estados miembros de la UE como destinatarios de esta norma (art. 24).

III. LA RESPONSABILIDAD POR PRODUCTOS TRANSFRONTERIZA POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL: ASPECTOS DE LEY APLICABLE

24. Una vez se ha dado cuenta del proceso que condujo a la elaboración de la Directiva (UE) 2024/2853, así como expuestos los elementos y novedades fundamentales que presenta este nuevo marco regulatorio para atender a los supuestos de responsabilidad derivada de productos en el nuevo contexto tecnológico y al respecto de los sistemas de IA, seguidamente se analizará la problemática que suscita la ordenación de tales casos, cuando cuenten con una naturaleza internacional. Y es que, como resulta plenamente comprensible, en la actualidad la actuación de los operadores económicos en este ámbito, la alta movilidad de los productos, así como del uso y los resultados relativos a los sistemas de IA, los daños que eventualmente ocasiones poseen frecuentemente un carácter internacional[89].

En este sentido, y sin desdeñar la importancia de la dimensión jurisdiccional —dominada en la actualidad por lo previsto en el Reglamento (UE) núm. 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Reglamento Bruselas I *bis*)[90]—, seguidamente se ofrecerá un estudio de esta problemática que, como se indicó desde la introducción, se centrará en la dimensión de la determinación de la ley aplicable en tales casos.

1. CUESTIONES INTRODUCTORIAS

25. Como se ha destacado, la ordenación de la IA desde la UE está llamada a contar con una destacada vocación internacional. De una parte, se ha de tener en cuenta que los objetivos de preservar el "constitucionalis-

88. Considerandos 60 y 61.
89. HAU, W. y KADNER GRAZIANO, T., "Products liability", *Encyclopedia of Private International Law*, Edward Elgar, Cheltenham (2017), Vol. 2, pp. 1413-1422, p. 1413; ORTEGA GIMÉNEZ, A.: *El Reglamento europeo…*, *op. cit.*, p. 14.
90. DO L 351/1 20 de diciembre de 2012.

mo digital" y la "soberanía digital" europea a los que atiende al esfuerzo regulatorio europeo en este sector, implica que estos posean una relevante proyección *ad extra*[91]. El cual suele relacionarse con el denominado "Efecto Bruselas"[92]. De otra parte, y ya en relación con los supuestos regulados por la Directiva (UE) 2024/2853, no van a ser infrecuentes los casos de responsabilidad derivada de productos defectuosos que cuenten con una naturaleza internacional. Una realidad de la que, además, se hace eco la propia Directiva.

De este modo, además de los eventuales litigios transfronterizos que pudieran tener lugar *ad intra* el mercado interior, ya en el Considerando 37 de la nueva Directiva se hace especial mención de la relevancia que posee su dimensión *ad extra* al destacar la necesidad de "garantizar que las personas perjudicadas tengan posibilidad de reclamar una indemnización exigible cuando un fabricante de un producto esté establecido fuera de la Unión".

26. Efectivamente, el art. 3.2 de la Directiva 85/374/CEE ya contemplaba esta circunstancia, al equiparar al importador a la figura del productor, afectando a su aplicación en supuestos de carácter transfronterizo[93]. No obstante, el nuevo marco regulador europeo toma una mayor conciencia de esta realidad y de su relevancia en el contexto tecnológico actual. De este modo, al regular la cuestión de los operadores económicos responsables de los productos defectuosos en su art. 8, recordar como en los casos en los que el fabricante —de un producto o componente— se encontrar establecido fuera de la UE, y al margen de la responsabilidad que le corresponda, el numeral 1, c) dispone que igualmente se considerará como operador a: "*i) el importador de un producto o componente defectuoso, ii) el representante autorizado del fabricante, y iii) cuando no haya un importador establecido en la Unión o un representante autorizado, el prestador de servicios logísticos*"[94]. A este respecto habrá que tomar en consideración asimismo lo previsto en el art. 11.1, a), la posibilidad de que el fabricante y el importador[95] puedan solicitar la exención de su eventual responsabilidad, si demuestran "*que no ha introducido el producto en el mercado ni lo ha puesto en servicio*".

---

91. GASCÓN MARCÉN, A.: "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", vol. 13, núm. 2, *CDT*, 2021, pp. 209-232, p. 232.
92. Por todos, BRADFORD, A.: *The Brussels Effect. How the European Union Rules the World*, Oxford University Press, Oxford (2020), pp. 131-169.
93. FRANCQ, S., *op. cit.*, p. 350.
94. Considerando 37.
95. Definido en el art. 4.12 como "*toda persona física o jurídica que introduzca en el mercado de la Unión un producto de un tercer país*". *Vid.* WENDEHORTS, C., *op. cit.*, pp. 153-154.

27. La Directiva de 2024, sin embargo, no establece previsión normativa alguna al respecto de estos supuestos cuando cuenten con una naturaleza internacional —ya se trate de situaciones *ad intra* la UE o relacionadas con terceros Estados—; limitándose a proponer soluciones armonizadas de carácter sustantivo[96]. Tal y como se observa la respecto de la Propuesta de Directiva de 2022[97], al igual que se guardan silencio sobre esta dimensión transfronteriza en los Reglamentos relativo a la seguridad general de los productos y relativo a las máquinas de 2023[98]. Una exclusión de las cuestiones propias del DIPr que, a pesar de su evidente potencial regulatorio en este ámbito, plantea numerosos interrogantes y no menos desafíos en términos de previsibilidad y de seguridad jurídica; afectando, de forma particular, a la determinación de la ley aplicable a los supuestos de responsabilidad civil en el ámbito de IA[99].

De este modo y por lo que hace a los supuestos de responsabilidad derivada de productos defectuosos, sigue el mismo modelo regulatorio planteado desde la Directiva 1985. Y ello, a diferencia de lo previsto en el Reglamento de IA, donde su art. 2.1 prevé el juego extraterritorial por medio de una norma de conflicto unilateral que delimita su ámbito de aplicación territorial; afectando así a los responsables de despliegue de los sistemas de IA que estuvieran establecidos en terceros Estados, cuando operasen en el mercado UE[100].

96. En el mismo sentido, HENCKEL, K., *op. cit.*, p. 215.
97. En esta misma línea, hay que poner de relieve como, mientras que en la propuesta de Directiva sobre responsabilidad en materia de IA de 2022 tampoco se atendía a la dimensión internacional de supuestos que regulaba, en el Informe con recomendaciones elaborado por el Parlamento Europeo sí que incorporó soluciones de naturaleza conflictual, como se contemplaba en su art. 9 al enfrentarse a la cuestión de las "Disposiciones nacionales sobre indemnización y plazo de prescripción".
98. HENCKEL, K., *op. cit.*, pp. 213-220.
99. FERNÁNDEZ ROZAS, J.C., *op. cit.*, p. 21; MERCHAN MURILLO, A.: "Retos Regulatorios en torno a la Inteligencia Artificial", *Pensar,* vol. 23, núm. 4, 2018, p. 1-13, p. 11; POESEN, M., Regulating Artificial Intelligence (AI) in the European Union (EU): Exploring the Role of Private International Law (March 11, 2022), en X, Recht in beweging — 29ste VRG-Alumnidag 2022 (Gompel&Svacina 2022), pp. 297-314, pp. 313-314 (disponible en SSRN: https://ssrn.com/abstract=3959643 or http://dx.doi.org/10.2139/ssrn.3959643).
100. *Vid.* Considerando 21. Sobre esta cuestión, CZERNIAWSKI, M.: *op. cit.*, pp. 2 y 12; GASCÓN MARCÉN, A.: *op. cit.*, p. 216; HENCKEL, K., *op. cit.*, pp. 208-210; LÓPEZ-TARRUELLA MARTÍNEZ, A.: "El futuro Reglamento de Inteligencia Artificial y las relaciones con terceros estados", *REEI*, núm. 45, 2023, pp. 1-29, p. 13; ORTEGA GIMÉNEZ, A.: "El ámbito de aplicación territorial del Reglamento de inteligencia artificial", en COTINO HUESO, L. y SIMÓN CASTELLANO, P. (Dirs.), *op, cit.*, pp. 123-136, p. 129. *Cfr.* LUTZI, T.: "Einseitigket statt Allseitigkeit als Strukturprinzip des Digitalen Binnenmarkts?", *IPrax* 2024, pp. 262-266, pp. 263-266.

De ahí que resulte razonable preguntarse sobre cómo van a regularse las situaciones de responsabilidad por productos defectuosos de carácter transfronterizo a partir de la publicación de la Directiva (UE) 2024/2853, con especial atención a los casos en los que el perjuicio se produjera por un sistema de IA. Pero, sobre todo, y ante su silencio, sobre el papel destacado que desempeña el DIPr en el contexto de la UE en estos supuestos y, en concreto, para concretar la ley estatal reguladora en los casos en los que posean un carácter internacional[101]. Una cuestión que no sólo posee relevancia en relación con los supuestos vinculados a terceros Estados —ante la eventual aplicación de su normativa al caso concreto—, sino también entre Estados miembros cuando se presente un elemento de extranjería en la relación en cuestión; toda vez que la armonización imperativa que propone la nueva Directiva (como la de 1985) —aun cuando no sea de mínimos, sino de máximos[102]— no contempla una aproximación legislativa plena en la materia y además permite que se mantengan ciertas discrepancias regulatorias a nivel *ad intra* de la UE[103].

28. No obstante su relevancia, la ordenación de esta cuestión resulta más compleja de lo que parece a simple vista. Así, no sólo relaciona con la tradicional problemática que se suscita en el contexto de la UE y que afecta de forma singular al ámbito de la responsabilidad civil, al respecto de las relaciones que mantienen los resultados derivados de la armonización material (cuya base legal se sitúa en el art. 114 del TFUE) y la unificación conflictual (siendo que el fundamento jurídico lo vemos en el art. 81 del TFUE) en el seno de la UE[104]. Sino que, a su vez, por lo que respecta a esta materia concreta, igualmente se vincula con la falta de uniformidad y la

101. CAPPIELLO, B., *op. cit.*, p. 148-152. *Vid.* KAYE, P., *Private International Law of Tort and Product Liability*, Datmouth, Aldershot (1991), pp. 108-109; TORRALBA MENDIOLA, E.C., *La responsabilidad del fabricante. Aplicación de la ley extranjera y normativa comunitaria*, Marcial Pons, Madrid (1997), pp. 39-62; SCHWARTZE, A., "A European regime on international product liability: Article 5 of Rome II Regulation", *NIPR,* 2008, pp. 430-434, p. 430.

102. Crítico, GÓMEZ LIGÜERRE, C., *op. cit.*, pp. 4-5. En relación con el marco normativo precedente, SEUBA TORREBLANCA, J.C., "Las Sentencias del Tribunal de Justicia de la Comunidades de 25 de abril de 2002 sobre la Directiva 85/374, de productos defectuosos: una directiva imperativa, no de mínimos", *InDret,* 2002.3, pp. 1-3.

103. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1413; MACHNIKOWSKI, P., "Article 5", en MAGNUS, U. MANKOWSKI, P (Eds.), *Rome II Regulation*, Otto Schmidt, Colonia (2019), pp. 211-230, p. 213; PALAO MORENO, G., "Product Liability: jurisdiction and applicable law in cross-border cases in the European Union", *ERA Forum,* 2010, pp. 45-65, p. 46.

104. PALAO MORENO, G., *Responsabilidad civil extracontractual en el Derecho europeo*, Tirant lo Blanch, Valencia (2008), pp. 58-66, 71-74 y 192-196.

complejidad normativa que se manifiesta desde esta perspectiva conflictual en el ámbito europeo —y con una incidencia particular para España—, al coexistir en estos momentos y por lo que hace a esta materia, tanto la solución especializada prevista en el art. 5 el Reglamento (CE) núm. 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales ("Roma II") (Reglamento Roma II)[105] y el Convenio de La Haya de 1973, sobre la ley aplicable a la responsabilidad por productos[106].

29. A este respecto, hay que tener presente que, partiendo del carácter universal tanto del Reglamento Roma II (que impone su art. 3), como del Convenio de La Haya de 1973 (en el art. 11), así como de lo previsto en el art. 28.1 del Reglamento Roma II (al establecer las relaciones entre ellos), se colige la actual vigencia del Convenio de La Haya de 1973, para los Estados miembros que lo hubieran ratificado con anterioridad a la entrada en vigor del Reglamento europeo —como así sucede con España—[107]. Un hecho del que se deriva, unido al hecho de que cuentan con un ámbito de aplicación material ciertamente similar —como se podrá apreciar seguidamente—, un efecto de fragmentación legal en este ámbito material y en relación con el mercado interior UE, tolerado por razón de que los Estados miembros signatarios respeten sus compromisos internacionales[108].

La mencionada coexistencia normativa en la regulación los aspectos conflictuales relativos a la responsabilidad por productos defectuosos y las disparidades sobre el régimen aplicable según el Estado miembro en cuestión, ha sido mecedora de crítica por la doctrina. Y ello, no sólo por entender que no logra favorecer la promoción de la uniformidad normativa en el contexto europeo, sino porque que además es susceptible de generar un indeseable nivel de previsibilidad e inseguridad jurídica para el operador económico que introduzca o comercialice sus productos en el mercado interior, pudiendo incluso llegar a fomentar prácticas de *forum shopping*[109]. De

105. *DO* L 199, de 31 de julio de 2007.
106. *BOE* núm. 21, de 25 de enero de 1989.
107. En la actualidad, son 11 los países parte del Convenio. Los Estados miembros de la UE que han ratificado el Convenio de La Haya de 1973 son: Croacia, Eslovenia, España, Finlandia, Francia, Holanda y Luxemburgo. *Vid.* GUZMÁN PECES, M., "La coordinación de normas de fuente internacional e institucional: la responsabilidad del fabricante por productos defectuosos", *AEDIPr,* 2011, pp. 695-716.
108. Considerando 36.
109. BRIÈRE, C., "Réflexions sur l'interaction entre la proposition de règlement 'Rome II' et les conventions internationales", *JDI,* 2005, pp. 677-694, pp. 693-694; DICKINSON, A., *The Rome II Regulation: the law applicable to non-contractual obligations*, Oxford University Press, Oxford (2008), p. 388; HELLNER, M., "The relationship between the Rome II

ahí que hubiera resultado aconsejable que, ya por arte de la UE y durante el proceso de elaboración del Reglamento Roma II, se hubiera atendido esta cuestión con el fin de evitar esta coincidencia normativa —o que se reconsideren las relaciones que mantienen en una futra revisión del Reglamento Roma II[110]—; o ya por parte de los Estados miembros que ratificaron en su momento el Convenio de La Haya de 1973, se hubiera procedido a denunciarlo con anterioridad a la entrada de aplicación del instrumento europeo —resultando una opción viable tras su entrada en vigor—. Una postura frente al Convenio que destaca como altamente recomendable que, sin embargo, e incomprensiblemente, no se ha planteado hasta la fecha por ninguno de los Estados miembros que son parte del mismo[111].

2. LA PROBLEMÁTICA QUE SUSCITA LA APLICACIÓN DEL CONVENIO DE LA HAYA DE 1973

30. Como consecuencia de lo expuesto, en tanto que Estado miembro al que le obliga el Convenio de La Haya de 1973, desde la perspectiva española debe llevarse a cabo un examen de este instrumento convencional, para comprobar su juego al respecto de los daños que, como productos defectuosos, pudiera ocasionar un sistema de IA. A este respecto, la primera cuestión que hay que tener presente al respecto del juego del Convenio de 1973, se relaciona con la determinación de su ámbito de aplicación y, sobre el mismo, su eventual juego al respecto de los supuestos de daños derivados de productos defectuosos ocasionados por sistemas de IA. Y ello, partiendo de su carácter universal como se ha destacado, aplicándose incluso en supuestos conectados con países no signatarios, sin poder exigirse condición de reciprocidad alguna.

Para empezar, el ámbito de aplicación material del Convenio se localiza en los arts. 1 a 3. Entre ellos destaca el 1.º que, en su apartado I dispone —con gran amplitud— su juego con relación a "*los daños causados por un producto,*

Regulation and the 1973 Hague Convention", *Oslo Law Review,* Vol. 6, núm. I, 2019, pp. 72-74; KADNER GRAZIANO, T., "Das auf ausservertragliche schuldverhältnisse anzuwende rect nach inkrafttreten der Rom II-Verordnung", *Rabels Z* 2009, pp. 1-77, p. 44; VON HEIN, J., "Forward to the Past. A Critical Evaluation of the European Approach to Artificial Intelligence in Private International Law", en VOENEKY, S. (Ed.), *The Cambridge Handbook of Responsible Artificial Intelligence. Interdisciplinary Perspectives*, Cambridge University Press, Cambridge (2022), pp. 2010-226, pp. 215-216.

110. SCHMID, C. y PINKEL, T., "Article 5. Product liability", en: CALLIES, G.P. (Ed.), *Rome Regulations*, Kluwer Law International, Alphen aan den Rijn (2011), pp. 431-459, p. 450.

111. HENCKEL, K., *op. cit.*, p. 224; VON HEIN, J., "Forward to the Past…", p. 215.

comprendidos los derivados de la descripción inexacta del producto o la falta de indicación adecuada de sus cualidades, características o modo de empleo". Eso sí, siempre que estos merezcan un carácter extracontractual, por razón de que la propiedad o el disfrute del producto causante del perjuicio no hubiere sido transferida al perjudicado por la persona a quien se le imputara la responsabilidad (como señala su párrafo II)[112]. Asimismo, no hay que perder de vista que el juego del instrumento no dependerá de la jurisdicción o de la autoridad que tuviera que conocer del litigio, como se subraya el apartado III.

31. De ahí que, los aspectos esenciales que hay que tomar en consideración para que pueda a las soluciones conflictuales previstas en el Convenio de 1973, se relacionan con la delimitación de tres conceptos principales:

a) Por un lado, la noción de "producto" se sitúa en el art. 2, a), y posee una gran relevancia para este análisis, ya que resulta de difícil aplicación a los sistemas de IA; al cubrir los productos naturales e industriales, ya fueran en bruto o estuvieran manufacturados, comprendiendo muebles o inmuebles —sin hacer mención alguna, como corresponde al momento de su elaboración, a bienes inmateriales, como podrían ser los programas de ordenador o los sistemas de IA[113]—.

b) Junto a ello, el art. 2, b) establece que por "daño" se entenderá todo tipo de perjuicio ocasionado a las personas o bienes, en un sentido amplio; incluyendo la pérdida económica, aunque excluyendo el daño al producto en sí y la pérdida económica correspondiente, a no ser que fueran unidas a otros daños.

c) Por último, y como contempla la concreción de las "personas" a las que se aplica el instrumento se relaciona con las físicas y jurídicas, como establece el art. 2, c); refiriéndose como sujetos responsables en el art. 3, a: los fabricantes de productos acabados o de componentes; los productores de productos naturales; los proveedores de productos; otras personas que interviniesen en la cadena comercial de preparación y distribución, incluidas las encargadas de reparar y de almacenar un producto; al igual que la responsabilidad de los agentes o empleados de las personas arriba señaladas[114].

112. *Vid*. REESE, W.L.M., "Explanatory Report", en: *Convention on the La Applicable to Products Liability, Actes et documents de la Douzième session (1972)*, T. III, Bureau Permanent de la Conférence de La Haye de droit international privé, The Hague (1974), pp. 253 y 257.
113. HENCKEL, K., *op. cit.*, p. 215.
114. REESE, W.L.M., "Explanatory Report", *op. cit.*, p. 254.

32. La falta de referencia a los bienes intangibles en el art. 2 del Convenio de La Haya de 1973 suscita la pregunta de si este instrumento resultaría aplicable a los supuestos de responsabilidad derivada de productos defectuosos en el contexto de la utilización de sistemas de IA. En efecto, la literalidad del precepto haría pensar su inadaptación a estos novedosos supuestos de daños y, por tanto, su inaplicación en estos casos. No obstante, hay que tener en cuenta que el propósito del Convenio fue la cobertura de todo tipo de daños, tal y como se deriva de lo expuesto en su *Explanatory Memorandum*[115]. Por lo que, a pesar de su referencia directa a bienes tangibles, y como subraya HENCKEL, resultaría razonable pensar que se encontrara en línea con el espíritu que orientó al legislador internacional en el momento de su elaboración afirmar su aplicabilidad a los daños ocasionados por programas de ordenador y sistemas de IA[116].

33. Delimitado su ámbito de juego, hay que enfrentarse a las soluciones conflictuales que recoge el Convenio de 1973, contendías principalmente en los arts. 4 a 7. Para su diseño el legislador internacional acudió a una metodología basada en el empleo de puntos de conexión plurales jerárquicamente estructurados, recurriendo al sistema de "agrupamiento de contactos"[117]; ofreciendo, de esta manera, una respuesta especializada y materialmente orientada que favorece el equilibrio de intereses entre personas perjudicadas y responsables[118], aunque por medio de una reglamentación un tanto compleja que jugaría en detrimento de un deseable nivel de previsibilidad legal[119]. De este modo, de su examen cabe destacar lo siguiente:

a) En primer término y como se aprecia de lo establecido en su inicio, resulta de aplicación el art. 5, estableciendo como criterio de conexión inicial (a pesar de su ubicación en el articulado) el de la residencia habitual de la persona que hubiera sufrido el perjuicio

115. *Ibid.*, pp. 253 y 257-258.
116. HENCKEL, K., *op. cit.*, p. 215-216.
117. REESE, W.L.M., "Explanatory Report", *op. cit.*, pp. 251-273.
118. ZABALO ESCUDERO, M.E. "La ley aplicable a la responsabilidad por daños derivados de los productos en el Derecho internacional privado español", *REDI*, 1991, pp. 75-107, pp. 90-94.
119. *Vid.* DE ANGULO RODRÍGUEZ, "El Convenio de La Haya sobre la ley aplicable a la responsabilidad por daños derivados de los productos", *ADC*, 1974, pp. 921-934, p. 934; FAWCETT, J.J., "Product liability in Private International Law: A European perspective", *Recueil des Cours* 1993-I (238), pp. 1-246, pp. 150-155; SARAVALLE, A., *Responsabilitá del produttore e dirittto internazionale privato*, Cedam, Padua (1991), p. 186; TEBBENS, H.D., *International products liability*, Sijthoff & Noordhoff, Alphen aan den Rijn (1979), p. 357.

directo del producto defectuoso —un criterio tecnológicamente neutro, aplicable sin grandes dificultades en los supuestos de daños ocasionados por la IA y que beneficiaría a este sujeto—; para los casos en los que fuera, a su vez, el país donde se localizase el establecimiento principal de la persona responsable o donde el perjudicado hubiera adquirido dicho producto —ambos perfectamente trasladables al nuevo contexto tecnológico, al igual que previsibles para las partes y procurando el equilibrio de sus intereses—[120].

b) En segundo lugar, según lo previsto en su art. 4, se acudirá al tradicional y territorial criterio basado en el lugar de producción del daño directo a la persona perjudicada —entendido como donde se manifestó por vez primera o produjo el primer impacto— (en tanto que *loci damni*); por tanto, claramente favorable al sujeto dañado (por su proximidad y previsibilidad para este sujeto) y que además resulta adaptable a los supuestos de daños producidos por IA (incluso en situaciones en línea), en atención a su neutralidad tecnológica; siempre y cuando éste coincidiera además, con el país donde se sitúe la residencia habitual de la persona perjudicada, se desarrollara la actividad principal de la persona responsable —como se ha indicado, criterios perfectamente adaptables a la nueva realidad tecnológica— o el lugar de la adquisición del producto[121].

c) En tercer lugar, caso de no resultar aplicables las respuestas anteriores, el art. 6 prevé la aplicación de la ley del país donde se sitúe el establecimiento principal del fabricante, permitiendo a la persona dañada optar por el ordenamiento del lugar de perjuicio en estos supuestos —ambos fácilmente adaptables al contexto de la IA y, en este caso, favoreciendo a los intereses del sujeto perjudicado—[122].

d) En todo caso y como se prevé en el art. 7, no se tomaría en consideración lo establecido en los tres preceptos anteriores, si la persona

120. *Vid.* HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1417; REESE, W.L.M., "Explanatory Report", *op. cit.*, p. 262.

121. Al respecto, HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1417; REESE, W.L.M., "Explanatory Report", *op. cit.*, pp. 254 y 260; TORRALBA MENDIOLA, E.C., *op. cit.*, pp. 85-86.

122. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1417. Aunque de difícil aplicación, por razón del efecto bloqueante que en la práctica va a desplegar los arts. 4 y 5, en opinión de ESTEBAN DE LA ROSA, G., "Ley aplicable a la responsabilidad por productos en Derecho internacional privado español", *RGD*, núm. 667, 2000, pp. 4363-4390, p. 4373.

> responsable no hubiera podido prever razonablemente que se produciría la comercialización del producto defectuoso o un producto del mismo tipo en tales países. Algo que, por lo que respecta a los sistemas de IA, exigiría de los operadores económicos la adaptación de sus procesos en supuesto de introducir tales productos en países distintos del de su establecimiento, pudiendo incluso limitar territorialmente los mercados estatales a los que dirigirlos. Una cláusula de "previsibilidad" que equilibra los intereses a favor de los del sujeto cuya responsabilidad se exige, siempre y cuando esta persona no hubiera "dirigido" sus actividades a los países resultes de aplicar las soluciones conflictuales previstas en los arts. 4 a 6 (proponiendo una suerte de "desconexión" de las mismas, por tanto)[123].

34. En otro orden de ideas, mientras que el articulo 8 delimita los extremos que entran en el ámbito de aplicación de la *lex causae*, el art. 9 se enfrenta al juego imperativo de las normas de seguridad propias del país en cuyo mercado se hubiera introducido el producto[124]. Por otra parte, la excepción de orden público se sitúa en el art. 10, no teniendo cabida el juego del reenvío en ningún caso al hacerse referencia a la aplicación del "derecho interno" en todos los casos[125]. Por último, los artículos 12 a 14 se enfrentan a las cuestiones de plurilegislatividad[126]. Sobre el resto de las cuestiones relativas a los problemas de aplicación de las normas de conflicto el Convenio guarda silencio, por lo que podría llegar a pensarse en acudir a las respuestas establecidas en el Reglamento Roma II para cubrir estas lagunas[127].

3. LAS POSIBILIDADES QUE OFRECE EL REGLAMENTO ROMA II

35. Aun cuando España se encuentra obligada en la actualidad por lo previsto en el Convenio de La Haya de 1973, el análisis de las soluciones incluidas en el Reglamento Roma II poseen una significativa importancia

123. REESE, W.L.M., "Explanatory Report", *op. cit.*, pp. 263-264; TORRALBA MENDIOLA, E.C., *op. cit.*, p. 98. Crítico, TEBBENS, H.D., *op. cit.*, pp. 357-358.
124. *Vid.* REESE, W.L.M., "Explanatory Report", *op. cit.*, pp. 255-256.
125. *Ibid.*, p. 256.
126. *Ibid.*, p. 256.
127. Tal y como podría ser, el daño del producto en sí mismo (art. 4), la acción directa contra el asegurador de la persona responsable (art. 18), la subrogación (art. 19) o incluso la posibilidad de elección de la ley reguladora de la responsabilidad (art. 14). En este sentido, CORNELOUP, S., "La responsabilité du fait des produits", en CORNELOUP, S. y JOUBERT, N. (Dirs.), *Le règlement communautaire "Rome II" sur la loi applicable aux obligations non contractuelles*, Litec, Paris (2008), pp. 100 y 104; MACHNIKOWSKI, P., *op. cit.*, p. 214.

en los supuestos de responsabilidad civil analizados. Entre otros motivos, por ofrecer un modelo regulatorio de origen europeo que obliga a la mayor parte de los Estados miembros de la UE, por la actualizada aproximación conflictual que contiene, por la relación tan directa que mantiene con el proceso armonizador de naturaleza material que en su momento condujo a la elaboración de la Directiva de 1985 y por su contribución a la previsibilidad y seguridad jurídica en este tipo de supuestos[128]. Una serie de motivos que, además de las mejoras que impone frente al Convenio de La Haya de 1973, deberían hacer reconsiderar al legislador español su posición en relación con el texto convencional[129].

36. Así las cosas, el Reglamento Roma II constituye un instrumento por medio del que se unifican las normas de conflicto de leyes para los Estados miembros y que resulta plenamente a los supuestos de responsabilidad civil derivados de productos defectuosos, siempre y cuando el ilícito civil ocasionado por un producto defectuoso entrara en su ámbito de aplicación. Una cuestión que, por lo que respecta a los supuestos relacionados con la A y, en principio, no suscitaría grandes dificultades en atención a lo dispuesto en sus arts. 1 a 3 —donde se establece el ámbito de aplicación material y territorial del instrumento europeo—, y que obligaría a analizar lo previsto en el art. 5 ("Responsabilidad por los daños causados por productos defectuosos").

A este respecto, el art. 5 del Reglamento Roma II contiene una norma de conflicto especializada y orientada materialmente que, además de promocionar, la previsibilidad, la certeza legal y limitar los supuestos de *fórum shopping*, para garantizar el buen funcionamiento del mercado interior, al igual que su aplicación coherente y compatible con las normas de jurisdicción presentes en el Reglamento Bruselas I *bis*[130] —como, con carácter general, se predica del Reglamento Roma II[131]—; persigue, en particular, alcanzar un equilibrio entre la tutela de los consumidores y la

128. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1422.

129. PALAO MORENO, G., "Product liability…", *op. cit.*, p. 62.

130. ILLMER, M., "The New European Private International Law of Product Liability — Steering Through Troubled Waters", *Rabels Z*, 2009, pp. 269-313, p. 309.

131. Considerandos 1-4 y 6. GARCIMARTÍN ALFÉREZ, F.J., "La unificación del Derecho conflictual en Europa: el Reglamento sobre ley aplicable a las obligaciones extracontractuales ('Roma II')", *La Ley*, núm. 6798, 2007, pars. 41-42; VON HEIN, J., "Forward to the Past…", pp. 211-212. *Cfr*. G. PALAO MORENO, "Las reglas generales relativas a la determinación de la ley aplicable a los hechos dañosos, a la vista de los objetivos del Reglamento europeo sobre ley aplicable a las obligaciones extracontractuales (Roma II)", en AA.VV., *Hacia un Derecho conflictual europeo: realizaciones y perspectivas*, Universidad de Sevilla, Sevilla (2008), pp. 65-80, p. 79.

predictibilidad empresarial por medio de un "justo reparto de los riesgos inherentes a una sociedad moderna caracterizada por un alto grado de tecnicidad, la protección de la salud de los consumidores, el incentivo a la innovación, la garantía de una competencia no falseada y la simplificación de los intercambios"[132].

37. En este sentido, al referirse a los supuestos de responsabilidad no contractual derivado de un daño causado por en productos —tanto de carácter objetivo, como por culpa[133]—, el legislador europeo procura alinear el concepto del "producto" que emplea el art. 5 Reglamento Roma II, al establecido en la 85/374/CEEC[134]. Por lo que, en línea de principio, la reformulación que ha sufrido este instrumento y, por tanto, del concepto de "producto" que utiliza la nueva Directiva (UE) 2024/2853, debería suponer un nuevo alineamiento del concepto que utiliza el Reglamento Roma II al nuevo contexto normativo sustantivo —en los términos explicados con anterioridad al analizar la nueva Directiva y, por tanto, cubriendo a los supuestos de IA—[135].

Aunque resulta de interés subrayar como dispone de un ámbito de juego incluso mayor que el presente en la Directiva de 2024, tanto desde una perspectiva objetiva, como subjetiva. Así, por lo que hace a la primera, el art. 5 cubriría los supuestos de responsabilidad objetiva y también por negligencia[136]. Junto a ello y al respecto de los sujetos perjudicados, el ámbito de juego personal que acoge el art. 5 al hacer referencia a las "*personas*",

132. Considerando 20. En esta línea, ILLMER, M., "Article 5. Product liability", en HUBER, P. (Ed.), *Rome II Regulation. Pocket Commentary*, Sellier, Munich (2011), pp. 113-142, pp. 116-118; PALAO MORENO, G., "Product liability…", *op. cit.*, p. 46; SARAVALLE, A., "The law applicable to products liability: hopping off the endless merry-go-round", en MALATESTA, A., (Ed.), *The unification of choice of law rules on torts and other non-contractual obligations in Europe. The "Rome II" proposal*, Cedam, Padua (2006), pp. 107-125, p. 111.

133. SCHMID, C. y PINKEL, T., *op. cit.*, p. p. 434.

134. CAPPIELLO, B., *op. cit.*, p. 145; HENCKEL, K., *op. cit.*, p. 215; LAFUENTE SÁNCHEZ, R., *op. cit.*, p. 203; MÜLLER-BERG, M.F., *op. cit.*, p. 225. *Vid.* VON HEIN, J., "Europäisches Internationales Deliktsrecht nach der Rom II-Verordnung", *ZEuP,* 2009, pp. 6-33, p. 26. *Cfr.* A. DICKINSON, *op. cit.*, p. 367; MACHNIKOWSKI, P., *op. cit.*, p. 216-217.

135. *Vid.* CAPPIELLO, B., *op. cit.*, p. 126; HENCKEL, K., *op. cit.*, p. 223; VON HEIN, J., "Forward to the Past…", p. 218. Sobre las dudas que suscitaba su posible juego para estos supuestos, con anterioridad a la reforma de la Directiva en 2024, el Informe elaborado por el BRITISH INSTITUTE OF INTERNATIONAL AND COMPARATIVE, *Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations*, European Union, Bruselas (2021), p. 34. También, POESEN, M., "Private International Law and Artificial Intelligence: An EU Perspective", *ERPL,* Vol. 31, núm. 2/3, 2023, pp. 365-386, p. 373.

136. MACHNIKOWSKI, P., *op. cit.*, p. 216.

incluiría a la persona dañada y a la responsable[137], incluyendo incluso a los transeúntes inocentes (*bystanders*), al igual que a aquellos sujetos que hubiera participado de modo activo en la producción o en la comercialización de los productos defectuosos[138].

38. No obstante, antes de proceder al análisis de este precepto se ha de dejar constancia de la posibilidad de que disponen las partes de seleccionar —de forma expresa o tácita— la ley rectora a este tipo de responsabilidad, en atención a lo previsto en el art. 14 del Reglamento Roma II, al no encontrase excluida tal posibilidad en el art. 5[139]. Una eventualidad que, a pesar de presentarse en escasas ocasiones en la práctica, no cabe duda de las ventajas que se derivarían de su empleo en los supuestos examinados —en términos de la seguridad jurídica y previsibilidad que proporcionaría su empleo—, sino que además no suscitaría especiales problemas en relación con los supuestos de responsabilidad civil derivada de IA[140], más allá de las dificultades que ocasionaría la prueba de la existencia de este acuerdo y la posibilidad de invocarlo[141], tal y como acontece y se reconoce en relación con aquellos pactos de sumisión que se manifestasen con un digital[142].

En todo caso, hay que tener presente que el *pactum de lege utenda* —en atención a lo previsto en su apartado 1, a)— únicamente podrá llevarse a cabo una vez manifestado el perjuicio —previsiblemente durante el procedimiento—[143]. Además, como se destaca en sus numerales 2.º y 3, este acuerdo no podrá tener por efecto excluir el juego de las disposiciones de carácter imperativo propias del ordenamiento estatal donde se localizaran todos los elementos pertinentes a la situación, como tampoco podrá evitar la selección de la legislación de un tercer Estado, la aplicación de este tipo

137. HUBER, P. y ILLMER, M., "International product liability. A commentary on article 5 of the Rome II Regulation", *Yearbook of Private international law,* 2007, pp. 31-47, p. 38.
138. KADNER GRAZIANO, T., "Das auf ausservertragliche…", *op. cit.*, p. 39.
139. BACH, I., "Article 14. Freedom of choice", en P. HUBER (Ed.), *Rome II Regulation. Pocket Commentary*, Sellier, Munich (2011), pp. 324-342; MANKOWSKI, P., "Article 14", en: MAGNUS, U. MANKOWSKI, P (Eds.), *op. cit.*, pp. 436-535.
140. CAPPIELLO, B., *op. cit.*, p. 185.
141. Desde una perspectiva jurisdiccional resulta de interés, con relación a los supuestos analizados, la STJUE de 7 de febrero de 2013, Asunto C-543/10, *Refcomp* (ECLI:EU:C:2013:62).
142. *Vid.* VON HEIN, J., "Forward to the Past…", p. 217. Al respecto, por lo que se refiere a los acuerdos de sumisión a favor de tribunales, su validez se ha afirmado en las SSTJUE de 21 mayo 2015, Asunto C-322/14, *ElMajdoub* (ECLI:EU:C:2015:334); y de 24 noviembre 2022, Asunto C-358/21, *Tilman* (ECLI:EU:C:2022:923).
143. *Vid.* AMORES CONRADI, M. y TORRALBA MENDIOLA, E., "XI Tesis sobre le estatuto delictual", *REEI,* núm. 8, 2004, pp. 1-34, p. 30; SCHWARTZE, A., *op. cit.*, p. 433.

de disposiciones que estuvieran contenidas en la normativa del foro que se hubiera ocupado de incorporar la Directiva 85/374/CEE —así como, tras su entrada en aplicación, la Directiva (UE) 2024/2853—[144].

Así las cosas, lo cierto es que a pesar de que no resulta frecuente que se produzca este recurso a la autonomía de la voluntad conflictual en las situaciones de daños derivados de productos defectuosos en la práctica[145], esta alternativa ofrece un positivo nivel de previsibilidad y de seguridad jurídica al perjudicado y al responsable en los supuestos de responsabilidad civil examinados que debe ser tenida en cuenta[146].

39. Ahora bien, además del juego de la autonomía de voluntad a la que se ha hecho referencia, igualmente resulta reseñable como en el numeral 1.º del art. 5, al enfrentarse a los supuestos en los que no se hubiera llevado la elección de ley, la respuesta que contiene jugará sin perjuicio de lo previsto en el art. 4.2. Según el cual, y en ausencia de pacto, se prevé la aplicación de la normativa estatal del país donde se situase la residencia habitual[147] común de las partes cuando se hubiera producido el daño[148]. Una respuesta conflictual que, debido a lo poco frecuente del recurso a la *electio iuris* en estas situaciones[149], podría llegar a implicar el acudir a la ley del tribunal que resultara competente para conocer de la acción de responsabilidad[150].

144. Una limitación a la posibilidad de elección de la ley por el carácter imperativo de la normativa sustantiva de origen europeo que es susceptible de contar con una destacada relevancia en el ámbito de la IA, como destaca POESEN, M., "Private International Law…", *op. cit.*, pp. 372-373.

145. FRÖHLICH, C.W., *The Private International Law of Non-Contractual Obligations According to the Rome-II Regulation*, Dr. Kovac, Hamburgo (2008), pp. 29-30.

146. AMORES CONRADI, M. y TORRALBA MENDIOLA, E., *op. cit.*, p. 30; S. CORNELOUP, S., *op. cit*., pp. 85-106, p. 101.

147. Un criterio que se delimita en el art. 23 del Reglamento. Sobre su delimitación y los problemas que suscita en relación con las personas físicas a las que no se refiere, FRÖHLICH, C.W., *op. cit.*, pp. 75-76; P. HUBER y M. ILLMER, *op. cit.*, pp. 40-41; P. STONE, "Der Vorschlag für die Rom II-Verordnung über das auf ausservertragliche Schuldverhältnisse anzuwende Recht", *The European Legal Forum,* 2004, pp. 213-230, p. 230; S.C. SYMEONIDES, "Rome II and Tort Conflicts: A missed Opportunity", *AJCL,* 2008, pp. 1-46, p. 36.
AMORES CONRADI, M. y TORRALBA MENDIOLA, E., *op. cit.*, p. 30; KADNER GRAZIANO, T., "Das auf ausservertragliche…", *op. cit*., p. 42.

148. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1414; MACHNIKOWSKI, P., *op. cit*., p. 226.

149. PALAO MORENO, G., *Responsabilidad civil…*, *op. cit*., pp. 370-375; SCHWARTZE, A., *op. cit.*, p. 431.

150. BACH, I., "Article 4. General rule", en: HUBER, P. (Ed.), *op. cit*., pp. 64-113, pp. 92-99; DICKINSON, A., *op. cit.*, pp. 378-380; PALAO MORENO, G., *Responsabilidad civil…*, *op. cit.*, p. 372.

Como se ha afirmado en relación con el Convenio de La Haya de 1973, la utilización de la residencia habitual como criterio localizador no debería suscitar problemas aplicativos en relación con los daños ocasionados en el contexto de la utilización de un sistema de IA, en atención a su carácter tecnológicamente neutro. Sin embargo, cuando se presenta como la común de las partes su juego dista de ser sencillo; ya que no hay que perder de vista el hecho de que, en este tipo de supuestos de responsabilidad y más en el ámbito de los prejuicios que pudiera ocasionar la IA, no sólo puede resultar complicado localizar este lugar en relación con el operador económico responsable, sino que además resulta poco habitual que posean su residencia habitual en el mismo país la persona que hubiera sufrido perjuicio y el responsable del daño[151].

40. Consecuentemente, fuera de los casos de elección de ley previsto en el art. 14 y cuando no pueda acudir a la *lex loci domicilii communis* contemplados el art. 4.2, será cuando haya que recurrir a las soluciones conflictuales incorporadas en el art. 5 del Reglamento Roma II. Un precepto que, aunque modernizado y mostrando un mayor nivel de complejidad[152], comparte una cierta similitud con la aproximación metodológica presente en el Convenio de La Haya de 1973 (antes examinado)[153]. Algo que contrasta, sin embargo, con la sencillez del art. 7.2 del Reglamento de Bruselas I *bis* que, desde una perspectiva jurisdiccional, atiende a este tipo de casos de responsabilidad civil y que, por tanto, puede llegar a comprometer su compatibilidad e interpretación coherente en supuesto de juego conjunto en situaciones litigiosas[154].

Así las cosas y en atención a lo dispuesto en las letras a) a c) del art. 5.1, y de forma jerarquizada, se aplicaría del siguiente modo[155]. En primer lugar (letra a), se acudiría la ley de la residencia habitual de la víctima cuando se produjo el daño en el momento del perjuicio; aunque únicamente resultará eficaz en aquellos supuestos en los que resultase coincidente con el país de comercialización del producto defectuoso causante del daño. En segundo término (letra b) y en defecto del criterio anterior, resultaría de aplicación la normativa del país donde se produjo la adquisición de este producto; igualmente si éste coincide con el lugar de su comercialización[156]. Por último (letra c), a falta de los criterios anteriores, se localizará donde se hubiera

151. CAPPIELLO, B., *op. cit.*, p. 191.
152. Crítico, VON HEIN, J., "Forward to the Past…", pp. 218-219.
153. VON HEIN, J., "Europäisches Internationales Deliktsrecht…", *op. cit.*, p. 25.
154. ILLMER, M., "Article 5. Product liability", *op. cit.*, pp. 140-142.
155. *Vid.* PALAO MORENO, G., "Product liability…", *op. cit.*, pp. 58-59.
156. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1415; MACHNIKOWSKI, P., *op. cit.*, p. 227.

producido el perjuicio; el cual, como en los otros supuestos previos, siempre que la comercialización del producto se hubiera llevado a cabo en tal lugar.

41. Por lo que hace a la aplicabilidad de estos criterios para los supuestos de daños derivados de sistemas de IA en supuestos transfronterizos, en tanto que productos defectuosos, no suscitaría excesivos problemas en la práctica. Aunque en algunos casos exigiría una interpretación teleológica de los criterios de conexión, para su adaptación a las particulares circunstancias que rodean los supuestos de IA —sobre todo, cuando los perjuicios se ocasionen en el medio digital—. En este sentido:

a) Para empezar, la residencia habitual de la persona perjudicada en el momento de producción del daño constituye un criterio fáctico y tecnológicamente neutro que resultar beneficioso para este sujeto por tratarse de su medio social (como ya se ha destacado al analizar el Convenio de La Haya de 1973). Además, este punto de conexión ofrece un elevado nivel de previsibilidad y de certeza a las partes, más aún al establecer el momento de la conexión. Por lo que, no debería suscitar mayores dificultades de localización en el contexto de los perjuicios ocasionados por la IA[157].

b) Por lo que hace al criterio del lugar de adquisición del producto —el cual, además, podría coincidir con el lugar de la residencia habitual de la persona perjudicada—, resulta igualmente previsible para las partes, resultando plenamente adaptable a la realidad de la IA en los supuestos en los que se recibió el producto de forma presencial[158]. Sin embargo, podrían llegar a suscitarse en algunos supuestos los mismos problemas de localización que se dan en el contexto del comercio electrónico directo[159] —tal y como como sucedería al respecto de las ventas a distancia realizadas por medios electrónicos de sistemas de IA adquiridos en línea—; pudiendo interpretarse que el lugar de adquisición del producto se localiza en el país donde se realiza su descarga o donde el sujeto perjudicado tiene acceso a tales bienes[160].

c) Por último, el recurso a la ley del lugar donde se produjo el perjuicio —concebido como *lex loci damni*, según el modelo del art. 4.1 del Reglamento de Roma II—, no debería causar especiales problemas de localización fuera de escenarios virtuales. Sin embargo, este criterio sí que sería susceptible

157. CAPPIELLO, B., *op. cit.*, pp. 189-190 y 195; MACHNIKOWSKI, P., *op. cit.*, pp. 226-227. *Vid.* DICKINSON, A., *op. cit.*, pp. 371-376.
158. SCHMID, C. y PINKEL, T., *op. cit.*, p. 445.
159. DE MIGUEL ASENSIO, P. A., *Derecho privado de internet*, Civitas Thomson Reuters, Madrid (2022) (6.ª ed.), pp. 1257-1258.
160. CAPPIELLO, B., *op. cit.*, p. 196; LAFUENTE SÁNCHEZ, R., *op. cit.*, p. 206.

de generar unas dificultades en su localización en contextos en virtuales, aunque similares a las que se suscitan en relación con la concreción del lugar del perjuicio en línea; pudiendo ubicarse este criterio, en el lugar donde se hubieran descargado o se tuviera acceso a los contenidos perjudiciales, aunque pudiendo generar el riesgo de una aplicación "en mosaico" de tantas leyes como lugares de manifestación del daño[161].

En resumidas cuentas y con carácter general, se puede afirmar que la localización de los criterios de conexión que utiliza el art. 5.1 —con los que se combina el de la comercialización del producto— no plantearía particulares dificultades, en aquellos casos en los que el prejuicio se ocasionase por un sistema de IA. Los cuales atienden, a su vez, a los intereses de la persona perjudicada, al conducir a un ordenamiento conectado a este sujeto, resultando igualmente previsible para el sujeto del que se reclama la responsabilidad. Consecuentemente, el resultado conflictual al que podría conducir este precepto en los supuestos analizados, como consecuencia de su coincidencia con alguno de los tres elementos expuestos, entronca directamente con los objetivos antes mencionados de lograr el equilibrio entre los intereses de las partes y favorecer la previsibilidad en cuanto a la determinación de la ley aplicable[162].

42. Junto a lo expuesto, mención especial merece la concreción del lugar de comercialización del producto, en tanto que constituye el único criterio que se repite en los tres escenarios a los que hace referencia el art. 5.1; poniendo así de manifiesto su gran relevancia para la localización de la ley rectora de estos supuestos de responsabilidad civil[163]. Un criterio cuyo

---

161. CAPPIELLO, B., *op. cit*., p. *Vid.* PALAO MORENO, G., "Derecho Internacional privado", en CLEMENTE MEORO, M. y COBAS COBIELLA, M.E. (Dirs.), *Derecho de Daños*, Tirant lo Blanch, Valencia (2021), Tomo II, pp. 2007-2078, pp. 2049-2050. Desde una dimensión jurisdiccional las SSTJUE, de 16 de julio de 2009, Asunto C-189/08, *Zuid-Chemie* (ECLI:EU:C:2009:475); y de 22 de febrero de 2024, Asunto C-81/23, *FCA Italy and FPT Industrial* (ECLI:EU:C:2024:165). La opción por la conexión *loci acti* —no prevista para el ámbito conflictual en los casos examinados— por contra, acercaría la regulación del supuesto de responsabilidad al país donde se encontrase establecido el fabricante y se hubiera elaborado el producto, como se apreció desde la dimensión judicial en la STJUE, de 16 de enero de 2014, Asunto C.-45/13, *Kainz* (ECLI:EU:C:2014:7).

162. FRANZINA, P., "Il regolamento 'Roma II' sulla legge applicabile alle obligación extracontrattuali", en AA.VV., *La Unión Europea ante el Derecho de la globalización*, Colex, Madrid (2008), pp. 299-370, p. 336; HUBER, P. y ILLMER, M., *op. cit*., p. 41.

163. KADNER GRAZIANO, T., "The law applicable to product liability: the present state of the law in Europe and current proposals for reform", *ICLQ*, 2005, pp. 475-488, p. 481; MACHNIKOWSKI, P., *op. cit*., p. 218. Cfr. ILLMER, M., "Article 5. Product liability", 130-137.

objetivo principal consiste en servir a los intereses del productor, al conectar el supuesto a un ordenamiento que pudo haber previsto. Así las cosas, el ligar de comercialización del producto puede entenderse, en atención a lo establecido por la jurisprudencia del TJUE y sirviendo a la previsibilidad del sujeto responsable —al determinar su "introducción en el mercado" al que se refiere la Directiva con el que guarda una cierta similitud[164]—, como aquel donde se llevó a cabo la distribución del producto o donde éste "*se pone en circulación cuando sale del proceso de fabricación establecido por el productor y entra en el proceso de comercialización quedando a disposición del público con el fin de ser utilizado o consumido*"[165].

Por loque hace a este estudio, el criterio de la comercialización del producto no debería suscitar mayores dificultades de localización al respecto de los supuestos de daños ocasionados por la IA, ya que resultaría suficiente determinar la incorporación efectiva del producto que ocasionó el perjuicio al flujo comercial (según la regla del *stream of commerce*) en un país o su puesta en circulación en un determinado mercado, para su localización[166]. En relación con ello, resulta de interés tener en cuenta que el empresario debería poder prever esta comercialización, así como que ésta se hubiera producido bajo su control y en el contexto de su red de distribución o ventas[167]. Por lo que, con el objeto de evitar situaciones imprevisibles para el empresario, como también para el sujeto perjudicado, el fabricante podría considerar incorporar limitaciones geográficas o lingüísticas en su estrategia comercial que le permitirían prever el alcance territorial de tal comercialización[168].

43. Junto a lo expuesto, el art. 5.1 establece, en su párrafo II, una "cláusula de previsibilidad" en atención a la que se contempla la aplicación del ordenamiento de la residencia habitual de la persona cuya responsabilidad se alegase "*si no podía prever razonablemente la comercialización del producto o de un producto del mismo tipo*"[169]. Una previsión inspirada en el art. 7 del Convenio de La Haya de 1973[170], que, a pesar de su escasa relevancia en la

164. Definido en el art. 4.8 como "*primera comercialización de un producto en el mercado de la Unión*". *Vid.* MACHNIKOWSKI, P., *op. cit.*, p. 221.
165. En esta línea, la STJCE, de 9 de febrero de 2006, en el Asunto C-127/04, *O'Byrne* (ECLI:EU:C:2005:349). *Vid.* STJUE, de 2 de diciembre de 2009, Asunto C-358/08, *Aventis Pasteur* (ECLI:EU:C:2009:744). *Vid.* SCHWARTZE, A., *op. cit.*, p. 431.
166. *Vid.* CAPPIELLO, B., *op. cit.*, pp. 195-196; LAFUENTE SÁNCHEZ, R., *op. cit.*, pp. 204-206.
167. SCHMID, C. y PINKEL, T., *op. cit.*, p. 440.
168. HENCKEL, K., *op. cit.*, p. 223; LAFUENTE SÁNCHEZ, R., *op. cit.*, p. 206.
169. AMORES CONRADI, M. y TORRALBA MENDIOLA, E., *op. cit.*, p. 29.
170. TORRALBA MENDIOLA, E.C., *op. cit.*, pp. 99-101.

práctica[171], entraría en juego cuando no pudiera acudirse a las soluciones presentes en el párrafo anterior[172].

Una solución que, en principio, tendría un fácil juego en relación con los daños ocasionados por la IA, además de que permitiría al operador adoptar las medidas apropiadas en sus operaciones a escala global para limitar efectos adversos imprevisibles[173]. Aunque, en todo caso, tendrá que ser examinada en atención a las circunstancias de cada caso[174]; a partir de la cual el legislador europeo procuraría fomentar el equilibrio de intereses —aunque sirviendo claramente a los de los propios de los fabricantes y, de forma, particular, en el ámbito de la IA—[175].

44. En todo caso, el numeral 2.º del art. 5 contempla la exclusión de las previsiones incorporadas en el apartado anterior, siempre que existiera una ley más estrechamente vinculada al caso en cuestión. Nos encontramos así ante una "cláusula de escape" que, con una aplicación excepcional, ofrecería una aproximación flexible basada en el principio proximidad y que exigiría la prueba de los elementos que conducirían a establecer tal conexión estrecha a la persona que la invocara[176]. De ahí que su incorporación haya sido objeto de críticas, por el indeseable nivel de imprevisibilidad que significa en la determinación de la ley aplicable a estos supuestos de responsabilidad al que puede conducir[177]. Sin embargo, no hay que perder de vista que el juego de la "cláusula de escape" en los casos de responsabilidad relacionado con los sistemas de IA, tanto fomentaría el juego de la *lex fori*[178], como permitiría atender a situaciones singulares como aquellas en las que se diera la existencia previa de un contrato entre los sujetos[179], las de responsabilidad del importador o del suministrador[180], o las de transeúntes inocentes (*bystanders*)[181].

---

171. HAU, W. y KADNER GRAZIANO, T., "Products liability", *op. cit.*, p. 1416.
172. F.J. GARCIMARTÍN ALFÉREZ, *op. cit.*, par. 43; VON HEIN, J., "Europäisches Internationales Deliktsrecht…", *op. cit.*, p. 28; P. HUBER y M. ILLMER, *op. cit.*, pp. 43-44.
173. CAPPIELLO, B., *op. cit.*, pp. 196-197.
174. ILLMER, M., "Article 5. Product liability", *op. cit.*, p. 138.
175. Sin embargo, SYMEONIDES, S.C., *op. cit.*, p. 36; KADNER GRAZIANO, T., "Das auf ausservertragliche…", *op. cit.*, p. 43.
176. ILLMER, M., "Article 5. Product liability", *op. cit.*, p. 139; LAFUENTE SÁNCHEZ, R., *op. cit.*, p. 205; MACHNIKOWSKI, P., *op. cit.*, pp. 229-230.
177. HAMBURG GROUP FOR PRIVATE INTERNATIONAL LAW, "Comments on the European Commission's Draft Proposal for a Council Regulation on the Law Applicable to Non-Contractual Obligations", *Rabels Z*, 2003, pp. 1-56, p. 18; HUBER, P. y ILLMER, M. *op. cit.*, p. 45.
178. FRÖHLICH, C.W. *op. cit.*, p. 44.
179. CAPPIELLO, B., *op. cit.*, p. 193; KADNER GRAZIANO, T., "Das auf ausservertragliche…", *op. cit.*, p. 40.
180. SCHWARTZE, A., *op. cit.*, p. 433.
181. ILLMER, M., *op. cit.*, p. 302; MACHNIKOWSKI, P., *op. cit.*, p. 230.

45. Por último, un análisis del art. 5 del Reglamento Roma II no debería dejar de lado, en todo caso, la relevancia que van a poseer en la disciplina legal de los casos de responsabilidad derivada de productos defectuosos, determinadas normas de aplicación contenidos en este instrumento europeo. Tal y como serían, entre otras, la toma en consideración de las reglas de seguridad y de comportamiento del lugar del hecho que diera lugar a la responsabilidad (art. 17), el juego de las disposiciones imperativas (art. 16) o de la excepción de orden público (art. 26)[182]. Un ámbito que, como se ha expuesto desde el inicio del trabajo, se encuentra cubierto por distintos Reglamentos elaborados en el contexto de la Estrategia digital europea —como los antes mencionados Reglamento 2023/988 relativo a la seguridad general de los productos y Reglamento 2023/1230 relativo a las máquinas— en incluso por el Propio Reglamento de IA.

IV. VALORACIÓN

46. La posibilidad de que los sistemas de IA ocasiones perjuicios a los particulares y a sus bienes, en tanto que eventuales productos defectuosos, ocasiona significativos retos jurídicos que el legislador de la UE ha tratado de atender, debido a sus significativas repercusiones, no ya únicamente para la consolidación del mercado interior y el mercado único digital, sino sobre todo en relación con los valores y derechos fundamentales europeos y el papel estratégico que rodea a esta tecnología disruptiva. Para ello, el legislador europeo ha desarrollado una destacada acción regulatoria durante los últimos años, cuyo resultado directo y más reciente ha sido la publicación de la Directiva (UE) 2024/2853, entre cuyas finalidades se incluye la principal de adaptar la precedente Directiva 85/374/CEE que deroga, al nuevo contexto tecnológico, incluida la IA.

Esta modificación normativa en materia de responsabilidad derivada de productos defectuosos posee importantes repercusiones para el DIPr, toda vez que estos supuestos de responsabilidad cuentan frecuentemente con un carácter internacional. Y ello, entre otros motivos, debido a que los operadores económicos relacionados con la IA cuyos productos acceden al mercado europeo, pueden encontrase establecidos fuera de la UE en numerosas ocasiones. En relación con esta constatación, y partiendo de la falta de uniformidad que se predica de la respuesta conflictual existente en el contexto de la UE en la

182. Tal y como podría acontecer, en su caso, en el caso de aplicar leyes que contemplen "daños punitivos". Considerando 32. SCHWARTZE, A., *op. cit.*, p. 433; PALAO MORENO, G., *Responsabilidad civil...*, *op. cit.*, pp. 339-340; SYMEONIDES, S.C., "Resolving punitive-damages conflicts", *YbPIL*, 2003, pp. 1-34.

actualidad —que se debate entre la aplicación del Convenio de La Haya de 1973 y el Reglamento Roma II, según el Estado miembro involucrado (siendo que, a modo de ejemplo, a España le sigue obligando el instrumento convencional mencionado)— se ha llevado a cabo el análisis de las soluciones de ley aplicable que contienen ambos textos, para evaluar las posibilidades de adaptación a los daños que son susceptibles de generar los sistemas de IA en tanto que productos defectuosos en supuestos transfronterizos.

47. En este sentido, la primera conclusión que se extrae de este examen conduce a poder afirmar que, con carácter general, el sistema de DIPr ofrece una respuesta que resulta adaptable a este tipo de casos de responsabilidad [183]. Por lo que, al menos en estos momentos, no se aprecia la necesidad de modificar la normativa reguladora de estos supuestos para proceder a su adaptación al contexto de la IA [184]. Algo que se aprecia, en mayor medida y con una más técnica normativa apropiada, en relación con el art. 5 del Reglamento Roma II —abundando así en la recomendación de que España denuncie el Convenio de 1973 o que, a fata de ello, el legislador UE tome en cuenta esta distorsión en el proceso de revisión del Reglamento Roma II—.

Un resultado positivo que, sin embargo, no evita que se deba recomendar, tanto una alineación de sus ámbitos de aplicación sustantivo —sobre todo al efecto de garantizar la aplicación de este precepto a los supuestos de daños ocasionados por productos defectuosos, como se definen en la Directiva—, al igual que se favorezca la interpretación de los puntos de conexión que se utilizan en el art. 5 de conformidad a las circunstancias que rodean a los casos de responsabilidad a la actividad en materia de IA. Algo que, en línea de principio, no debería suscitar mayores dificultades —incluso en situaciones desarrolladas en línea y vinculadas al mercado digital—, pero que podría aconsejar prestar atención, de forma señalada, a la concreción de los criterios que se emplean en los textos analizados a la luz de la realidad que impone la IA. Las páginas precedentes, por tanto, contienen sugerencias interpretativas de como estos elementos, con la finalidad de que respondan adecuadamente a los desafíos que entraña la imparable incorporación de los sistemas de IA en nuestra vida diaria desde el sistema de DIPr propio los Estados miembros de la UE.

183. También, POESEN, M., "Private International Law…", *op. cit.*, pp. 375, 383 y 385; ŚWIERCZYŃSKI, M., "Artificial Intelligence in Private International Law", en: LAI L. y ŚWIERCZYŃSKI M. (Eds.), *Legal and technical aspects of artificial intelligence*, Varsovia, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, 2021, 162-171, p. 166.

184. En un sentido similar, el reciente Informe de la Comisión "sobre la aplicación del Reglamento (CE) n.º 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales (Reglamento Roma II)" (COM (2025) 20 final), p. 9.

Capítulo 7

Inteligencia Artificial y tutela jurídica de derechos digitales en la Unión Europea*

Isabel Reig Fabado
Prof.ª Titular de Derecho internacional privado
Universitat de València

SUMARIO: I. INTRODUCCIÓN. 1. *La Unión Europea en su afán regulador del entorno digital*. 2. *Los modelos generales de IA*. II. LA REGULACIÓN DE LOS RIESGOS SISTÉMICOS EN LA UE. 1. *Riesgos sistémicos en el Reglamento de IA*. 1.1. Introducción. 1.2. La clasificación de los riesgos sistémicos en el Reglamento de IA. 1.3. Las obligaciones adicionales para los riesgos sistémicos en el Reglamento de IA. 2. *Los riesgos sistémicos en la DSA*. 2.1. Categorías de riesgos sistémicos en la DSA. 2.2. Evaluación y mitigación de riesgos sistémicos en la DSA. A. La evaluación de riesgos sistémicos en la DSA. B. Las medidas de mitigación de riesgos sistémicos de la DSA. 2.3. Los procedimientos formales iniciados por la Comisión contra las grandes plataformas por incumplimiento de las obligaciones de la DSA. 3. *La aplicación conjunta de ambos Reglamentos*. III. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

1. LA UNIÓN EUROPEA EN SU AFÁN REGULADOR DEL ENTORNO DIGITAL

Ante una *sociedad digitalizada masivamente y una economía plataformizada*[1] en la que el número de personas conectadas globalmente asciende a cinco

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro la autora.

1. *Vid.* BURI, I., VAN HOBOKEN, J.: "La propuesta de Ley de Servicios digitales (DSA): una visión crítica", *DSA Observatory*, Instituto de Derecho de la Información (IVIR),

mil millones y medio, los desafíos que se presentan son múltiples y de muy diversa índole. Este avance en progresión geométrica implica un uso generalizado de los modelos y sistemas de inteligencia artificial (IA) por parte de las grandes plataformas digitales y los grandes motores de búsqueda para el tratamiento y difusión de contenidos. Esta utilización de la IA por las grandes plataformas afecta tanto a los sistemas algorítmicos de control o moderación y recomendación o curación de contenidos, como a los modelos de IA generativa, también, para la creación de contenidos.

Precisamente, la combinación de los dos elementos —el uso de IA y las grandes plataformas digitales— en el tratamiento de *contenidos* en línea deriva en una proyección exponencial de sus consecuencias, que presenta grandes ventajas, como la eficacia y la rapidez de las respuestas automatizadas, pero también inconvenientes. Como, por ejemplo, sesgo y errores de resultado, que generan problemas como la desinformación y la discriminación y que conculcan derechos fundamentales de los ciudadanos de manera *masiva*[2]. En efecto, cuando los resultados no deseados de estos problemas afectan a los derechos fundamentales o a la sociedad en su conjunto, pueden clasificarse como *riesgos sistémicos.*

Bajo un panorama político incierto y más bien convulso, la Unión Europea, que no es líder tecnológico y que apenas tiene una representación significativa en el sector de las grandes plataformas digitales, ha decidido mantenerse en su determinación de configurarse como el primero, y si no el primero, el más riguroso, de los marcos legislativos reguladores para el mercado y los usuarios digitales en la UE[3].

Consecuentemente, y al hilo de lo que se ha dado en denominar el "paquete digital", la UE ha publicado el Reglamento sobre IA que entró

Universidad de Ámsterdam, Documento de debate, octubre de 2021, 80 pp., esp. p. 4 (traducción propia), KAUSHAL, R., VAN DER KERKHOF, C., GOANTA, C., SPANAKIS, G. Y IAMNITCHI, A.: "Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database", 2024, en https://doi.org/10.48550/arXiv.2404.02894 y WILMAN, F.: "The Digital Services Act (DSA): An Overview", *SSRN, Comisión Europea*, diciembre 2022, en http://ssrn.com/abstract_4304586 (consultado el 15 de abril de 2025).

2. *Vid.* LLANO ALONSO, F.: *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Valencia, Tirant lo Blanch, 2024, esp. P. 189.

3. El propio ex Comisario Breton afirmaba a la época que "la UE es la primera jurisdicción del mundo en que se establece una norma completa para regular el espacio digital". *Vid.* la Declaración 22/4227 de la Comisión Europea en el Blog del Comisario BRETON, T.: "Sneak peek: how the Commission will enforce the DSA & DMA", de 5 de julio de 2022.

en vigor en agosto de 2024 y que prevé un período de implementación (en el sentido de aplicación efectiva de sus normas) de dos años[4]. Y ello tras la elaboración — entre otros instrumentos elaborados y también en fase de propuesta[5]— del Reglamento de Servicios Digitales (DSA)[6], bajo la finalidad de regular los problemas que plantean las prestaciones de servicios digitales y de armonizar, o mejor, unificar, las prerrogativas de estos servicios de intermediación digital en el ámbito de la Unión Europea[7]. En definitiva, esta normativa europea viene a proteger al usuario eliminando los denominados de modo genérico como *contenidos ilícitos*, a través de unas obligaciones de diligencia que deben cumplir las plataformas digitales. Estas obligaciones responden al deber de diligencia de estos operadores digitales y añaden unas obligaciones adicionales para las plataformas digitales de muy gran tamaño en el caso de riesgos sistémicos[8]. A mayor abundamiento, la UE ha establecido un régimen de general aplicación en el territorio de los Estados

4. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican los Reglamentos (CE) 300/2008, (UE) 167/2013, (UE) núms. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). *Vid.* por todos, DE MIGUEL ASENSIO, P. A.: "Propuesta de Reglamento sobre inteligencia artificial", *La Ley Unión Europea*, número 92, 2021.
5. Sobre todo, el Reglamento correlativo sobre Mercados digitales (DMA), el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (Texto pertinente a efectos del EEE), DOUE, de 12 de octubre de 2022, L 265, pp. 1-66.
6. Reglamento (UE) 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) (Texto pertinente a efectos del EEE), DOUE, de 27 de octubre de 2022, L 277, pp. 1-102. Aunque el Reglamento entra plenamente en vigor el 17 de febrero de 2024, se aplicaba con anterioridad a las plataformas en línea de muy gran tamaño y buscadores en línea de muy gran tamaño designadas como tales por la Comisión. *Vid*, CASTELLÓ PASTOR, J.J.(Dir.): "Análisis del Reglamento (UE) y su interrelación con otras normas de la Unión europea", Aranzadi, 2024.
7. La propia DSA afirma que lo que pretende es "armonizar plenamente las normas aplicables a los servicios intermediarios en el mercado interior con el objetivo de garantizar un entorno en línea seguro, predecible y digno de confianza y aborda(r) (…) los riesgos (…), (protegiendo) eficazmente los derechos fundamentales (…) y (facilitando) la innovación". *Vid. el Considerando número 9 del Reglamento de Servicios Digitales, op. cit., supra*, p. 33.
8. *Vid.* BROADVENT, M.: "The Digital Services Act, the Digital Market act, and the New Competion Tool", *Center for Strategic and International Studies*, nov., (2020), publicado en https://apo.org.au/node/309351 y FELIU ÁLVAREZ SOTOMAYOR, S.: "Ámbito territorial y aplicación del principio de control en origen en el Reglamento UE de ser-

miembros, en tanto en cuanto, será de aplicación a todos los intermediarios que presten sus servicios a usuarios de la Unión Europea, sin tener en cuenta su país de establecimiento[9].

En este marco jurídico y, específicamente, ambos instrumentos reguladores, tanto el Reglamento de Servicios Digitales (o DSA), como el Reglamento de Inteligencia Artificial (IA), abordan los riesgos sistémicos para la consecución de un entorno digital seguro y justo. De suerte que resulta necesario el establecimiento de una normativa de control con respecto a la reducción y eliminación de contenidos ilícitos digitales y de protección del usuario. El hecho es que las grandes plataformas digitales actúan como intermediario entre los diferentes usuarios ejerciendo una función continua de control de acceso que puede derivar en una relación de dependencia con el resto de operadores digitales[10]. Lo cierto es que, en definitiva, tanto la plataforma digital de gran tamaño, como los algoritmos o modelos generales de IA (así como también los sistemas de IA generativa) —que potencian exponencialmente sus capacidades y, en realidad, se retroalimentan— se encuentran en manos exclusivamente de cinco o seis —si no, menos— grandes corporaciones. La cuestión será establecer unas herramientas adecuadas, desde el punto de vista democrático, de control de las mismas.

Esta es la circunstancia que explica la firme determinación de la UE de establecer un marco jurídico normativo que pretende hacer frente a estos gigantes digitales, y cuyas normas son las primeras en aplicarse. Entes a los que se les otorga una excesiva discrecionalidad para la restricción y eliminación de contenidos ilícitos en red[11], bajo la prescripción general de la diligencia debida, teniendo en cuenta que puede producirse la vulneración de derechos fundamentales. No solo el derecho a la libertad de expresión, la intimidad, la imagen o la integridad moral, sino también, otros como el derecho a la información o a la pluralidad de medios de comunicación y

vicios digitales" en CASTELLÓ PASTOR, J.J.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 41-64.

9. *Vid.* BURI, I., VAN HOBOKEN, J.: "La propuesta de…", *op. cit. supra*, p. 22.

10. *Vid.*, entre otros, GRAFANAKI, S., "Platforms, the First Amendment and Online Speech: Regulating the Filters", *Pace Law Review*, volume 39, (2018) y HOLT, D. y HAMMEKE, F., *Two-Sided Markets, Platforms and Network Effects, E-Commerce Competition Enforcement Guide*, 2.ª ed., (2019).

11. De suerte que "(l)as plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño (…) deben evaluar los riesgos sistémicos que entraña el diseño, funcionamiento y uso de sus servicios, así como los posibles usos indebidos por parte de los destinatarios de estos servicios, y deben adoptar medidas de reducción de riesgos apropiadas respetando los derechos fundamentales". *Vid. el Considerando número 79 del Reglamento de Servicios Digitales.*

otros problemas derivados de la desinformación. Añadiendo que son estos entes privados los que tienen que definir en qué consisten estos contenidos ilícitos y nocivos no armonizados, lo cual supone mayor controversia a la problemática planteada[12].

En definitiva, la UE parece querer abordar la regulación del complejo fenómeno de la utilización de modelos de IA de uso general por las grandes plataformas digitales con especial referencia en los riesgos sistémicos. Esto es, una regulación complementaria, como veremos, básicamente, entre el Reglamento de IA y el Reglamento de Servicios digitales. Un modelo que pretende controlar los efectos negativos de esta tecnología sobre los derechos fundamentales o la sociedad en su conjunto. Teniendo en cuenta las dificultades que ya suponía la intervención de las plataformas de muy gran tamaño en la intermediación de la prestación de servicios digitales (Reglamento de Servicios digitales) y pensando cómo el uso de los modelos de IA de uso general, por parte de estos gigantes, puede agravar exponencialmente estos problemas (Reglamento de IA). Asimismo, el impacto de la implantación de esta normativa no solo pretende regular el juego en el mercado digital de la UE, sino que podría tener consecuencias extracomunitarias —*efecto Bruselas*— si fuera de incorporación para todas las operaciones o incluso se introdujera la normativa en otros ordenamientos jurídicos[13].

---

12. Tal es así que la propia DSA establece que "respeta los derechos fundamentales reconocidos en la Carta y los derechos fundamentales que constituyen principios generales del Derecho de la Unión. En consecuencia, el presente Reglamento ha de interpretarse y aplicarse de conformidad con tales derechos fundamentales, incluida la libertad de expresión e información, y la libertad y el pluralismo de los medios de comunicación. En el ejercicio de las competencias establecidas en el presente Reglamento, todas las autoridades públicas implicadas deben alcanzar, en situaciones en las que los derechos fundamentales pertinentes entren en conflicto, un equilibrio justo entre los derechos afectados, de conformidad con el principio de proporcionalidad". *Vid.* el Considerando número 153 del Reglamento de Servicios Digitales. Para un análisis en profundidad, *vid.* CASTELLÓ PASTOR, J.J.: "Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (p2b): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea" en CASTELLÓ PASTOR, J.J.(Dir.): Análisis del Reglamento de servicios digitales y su interrelación con otras normas de la Unión Europea, Aranzadi, 2024, versión digital.

13. Esta circunstancia ha sido señalada por algunos autores que refieren la globalización de este modelo, no solo introduciéndolo en las normativas de terceros ordenamientos jurídicos, sino también con la incorporación general por parte de estos gigantes digitales de los parámetros de moderación, curación y creación de contenido de esta normativa europea. A modo de ejemplo, podría tratarse de las obligaciones relativas a la transparencia o los mecanismos de resolución de disputas, así como las condiciones generales o los informes anuales. *Vid.* CHANDER, A.: "When the Digital Services Act Goes Global", *Berkeley Technology Law Review*, 2023, 19 pp., esp. p. 3, BRADFORD, A.:

De modo que el objeto de análisis de este trabajo consiste, pues, en hacer una aproximación al modo en que la UE ha decido abordar las grandes plataformas, especialmente, en el uso de la IA por lo que refiere a la evaluación y mitigación de riesgos sistémicos, en tanto en cuanto supone la eventual defensa de los derechos digitales de cientos de millones de personas en la UE y tiene, además, vocación de proyección global.

2. LOS MODELOS GENERALES DE IA

La utilización de IA por las grandes plataformas supone una herramienta de enorme impacto para la difusión y tratamiento de contenidos mediante el uso de datos y la generación de contenido. De modo que, en general, los sistemas algorítmicos de toma de decisiones automatizadas o de verificación de datos, que utilizan estos grandes operadores ejercen funciones de control, lo que se denomina moderación proactiva, y la función de curación o recomendación, que pueden dar lugar a errores de resultado o de sesgo. Mientras que los sistemas de inteligencia artificial generativa se utilizan por las grandes plataformas en la creación de contenidos (*deepfakes* y *bots*, por ejemplo) con capacidad para difundir información falsa y, en consecuencia, producir desinformación, con una relevancia especial, como riesgo sistémico y como se verá, en los procesos electorales.

El Reglamento de IA se aplica a los modelos de IA de uso general y a los modelos de IA de uso general que impliquen riesgos sistémicos, una vez se introduzcan en el mercado[14]. Esto es, cuando los modelos o sistemas

"The European Union in a globalized world: 'The Brussels Effect'", *Revue Européenne du Droit*, 75, 2, marzo de 2021, p. 2, LAPIEDRA ALCAMÍ, R., "Hacia la transparencia y la equidad en el *ranking* de resultados a la luz del Reglamento 2019/1150" en CASTELLÓ PASTOR, J.J. (Dir.): *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi (Thomson Reuters), 2021, pp. 161-193 y BARRIO ANDRÉS, M.: "El efecto Bruselas del Reglamento europeo de inteligencia artificial", *Otrosí, Revista de Colegio de abogados de Madrid*, núm. 2. 2024, pp. 47-48. Asimismo, tampoco puede perderse el riesgo inverso que se ha señalado como el *Test Puti*n, esto es, que determinadas democracias *imperfectas*, como India, Nigeria o Brasil, además de Rusia, incorporen en sus legislaciones internas versiones de esta normativa, utilizándolas para combatir la disidencia y el discurso de la oposición y favoreciendo el discurso político favorable al gobierno. *Vid.* BARATA MIR, J.: "Libertad de expresión…", *op. cit. supra,* esp. pp. 101.

14. En efecto, las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse una vez éstos se hayan introducido en el mercado. De modo que no serán de aplicación cuando un modelo propio se utilice en procesos internos que no se requieran para suministrar un producto o un servicio a un tercero y no se vean afectados los derechos de las personas físicas. *Vid.* el Considerando núm. 97 del Reglamento de IA.

de inteligencia artificial de uso general tengan efectos negativos sobre los derechos fundamentales o la sociedad en su conjunto. Como la inteligencia artificial utilizada se difunde por grandes plataformas digitales, en lo referido al tratamiento o generación de contenidos, consecuentemente, el marco jurídico de la UE (sobre todo, el Reglamento de inteligencia artificial) se complementa con el Reglamento de servicios digitales o DSA, como se expone con posterioridad. Tanto en lo que afecta al tratamiento de datos, como en lo referente a la generación de contenidos, cubierto por el Reglamento de inteligencia artificial. A tal efecto, conviene reseñar en qué consiste un modelo de IA general, por comparación con los sistemas de IA, y cuándo pueden entrañar riesgos sistémicos, que se desarrolla a continuación. La aproximación a la definición de un modelo de IA de uso general debe hacerse en función de sus características funcionales esenciales, esto es, de la generalidad y la capacidad de llevar a cabo de manera competente una amplia gama de tareas diferenciadas. Si bien los modelos de IA de uso general son elementos esenciales que componen los sistemas de IA, no se configuran por sí mismos como sistemas de IA, sino que requieren de la añadidura de otros componentes —como por ejemplo un interfaz de usuario— para poder ser considerados como sistemas de IA.

II. LA REGULACIÓN DE LOS RIESGOS SISTÉMICOS EN LA UE

1. RIESGOS SISTÉMICOS EN EL REGLAMENTO DE IA

1.1. Introducción

Los modelos de IA de uso general referenciados pueden, además, generar riesgos sistémicos. Piénsese en cualquier efecto negativo real o razonablemente previsible sobre accidentes graves, sectores críticos, salud y seguridad públicas, economía o procesos democráticos, así como, la difusión de contenidos ilícitos, falsos o discriminatorios[15].

Debido a su potencial para causar efectos negativos importantes, los modelos de IA de uso general con riesgo sistémico deben estar siempre sujetos a las obligaciones establecidas en el Reglamento de IA. No puede perderse de vista que el alcance y la capacidad de estos modelos de IA de uso general pueden aumentar exponencialmente la concurrencia de riesgos sistémicos. Circunstancia que ya se contemplaba en el Reglamento de Servicios digitales y que ahora el Reglamento de IA viene a complementar, por lo que se refiere a estos modelos.

15. *Vid.* el Considerando núm. 110 del Reglamento de IA.

Lo cierto es que, a lo largo del ciclo de desarrollo y debido a una amplia variedad de circunstancias —incluso de desarrollo futuro—, estos modelos pueden dar lugar a sesgos dañinos y discriminación que produzcan una reacción en cadena y afecten de manera masiva a las personas individualmente o de manera colectiva (toda una comunidad, una ciudad entera, determinados colectivos, etc.). Asimismo, también pueden favorecer la desinformación y conculcar el derecho a la intimidad y a los valores democráticos y los derechos humanos bajo un gran impacto.

Debido a todas las circunstancias concurrentes la clasificación de modelos de IA de uso general con riesgos sistémicos requiere una tarea compleja de evaluación. En principio, el Reglamento establece una presunción inicial de coma flotante junto con unos parámetros consensuados por los operadores —Oficina de IA, científicos, industria, sociedad civil y otros expertos— que midan su capacidad y alcance de gran impacto. Complementariamente, la Comisión puede designar el riesgo sistémico de un modelo de IA de uso general a través de una decisión individual que tendrá que evaluar globalmente los criterios especificados en el Anexo 13 del Reglamento de IA. Estos criterios refieren la calidad o el tamaño de los datos de entrenamiento, el número de usuarios profesionales y/o finales, sus modalidades de entrada y salida, su nivel de autonomía y escalabilidad y otros parámetros de medición de su capacidad y alcance de posible gran impacto[16].

Una vez determinado el riesgo sistémico de un modelo de IA de uso general, los proveedores del mismo estarán sujetos, además de las obligaciones generales, a unas obligaciones adicionales de evaluación y mitigación de riesgos sistémicos y de garantía de un nivel adecuado en materia de ciberseguridad. Medidas que incluyen, asimismo, el deber de información y notificación, así como el de transparencia. El Reglamento de IA señala, en este punto, la importancia de los Códigos de buenas prácticas que deben consensuarse y actualizarse por todos los operadores y deben contener las obligaciones de los proveedores, la taxonomía de riesgos y las medidas concretas de evaluación y reducción de riesgos sistémicos[17].

1.2. La clasificación de los riesgos sistémicos en el Reglamento de IA

El artículo 51 del Reglamento de IA contiene las reglas para la clasificación de los modelos de IA de uso general como modelos con riesgo sistémico. A tal efecto, se exige la concurrencia de algunas de las condiciones enumeradas en dicho precepto.

16. *Vid.* el Considerando núm. 118 del Reglamento de IA.
17. *Vid.* el Considerando núm. 116 del Reglamento de IA.

La primera condición consiste en que el modela tenga *capacidades de gran impacto que* sean evaluadas con las herramientas y parámetros técnicos de referencia (artículo 51.1.a del reglamento de IA). El párrafo segundo añade una presunción para este supuesto bajo la que se considera la concurrencia de capacidades de gran impacto, cuando la cantidad acumulada de cálculo para su entrenamiento, medida en operaciones de coma flotante, sea superior a 10 elevado a 25.

La segunda posibilidad, en el artículo 51.1.b, permite a la Comisión emitir una decisión (de oficio o a instancia de un grupo de expertos científicos[18]) que declare el riesgo sistémico del modelo de IA de uso general de modo *equivalente* al anterior, en atención a los criterios del Anexo XIII del Reglamento. En este sentido, los siete criterios contenidos en este Anexo refieren, entre otros, al número de parámetros del modelo, a la calidad o el tamaño del conjunto de datos o el número de usuarios profesionales o finales[19]. Se añade la posibilidad de que la Comisión adopte actos delegados con el objeto de actualizar los umbrales y los parámetros para adaptarlos a los avances tecnológicos.

---

18. En este sentido, *vid*. el artículo 90 del Reglamento de IA relativo a las alertas del grupo de expertos científicos sobre riesgos sistémicos.
19. El Anexo XIII del Reglamento de IA, bajo el título: "Criterios para la clasificación de los modelos de IA de uso general con riesgo sistémico a que se refiere el artículo 51", establece: "Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos equivalentes a los contemplados en el artículo 51, apartado 1, letra a), la Comisión tendrá en cuenta los siguientes criterios:
    a) el número de parámetros del modelo;
    b) la calidad o el tamaño del conjunto de datos, por ejemplo, medidos a través de criptofichas;
    c) la cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;
    d) las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);
    e) los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;
    f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la Unión;
    g) el número de usuarios finales registrados".

En cuanto al procedimiento, el Reglamento prevé en el artículo 52 la obligación para los proveedores de notificar a la Comisión la concurrencia de un modelo de IA de uso general con riesgo sistémico en el sentido del artículo 51.1.a que acabamos de referir. Para ello establece un plazo de máximo de dos semanas y dicha notificación incluye el deber de información al respecto.

Complementariamente, para el caso en el que dicha circunstancia no haya sido comunicada, la Comisión puede emitir una decisión que declare el modelo con riesgo sistémico. Conviene recordar que la Comisión también puede declarar el riesgo sistémico de un modelo (de oficio o a instancia de un grupo de expertos científicos[20]), teniendo en cuenta los citados criterios del Anexo XIII del Reglamento de IA. La Comisión puede reevaluar esta designación cada seis meses previa solicitud de los proveedores. Asimismo, velará por la actualización de los criterios y publicará una lista de modelos de IA de uso general con riesgo sistémico que mantendrá, de igual modo, actualizada.

1.3. Las obligaciones adicionales para los riesgos sistémicos en el Reglamento de IA

La Sección 3 del Reglamento de IA, en su artículo 55, contiene las obligaciones adicionales de los proveedores de modelos de IA de uso general con riesgo sistémico. Ello significa que los proveedores de estos modelos también deben cumplir con las obligaciones generales de los artículos 53 y 54 del Reglamento de IA. Las obligaciones adicionales para los riesgos sistémicos refieren las obligaciones de información y notificación, el deber de transparencia además de garantizar un nivel adecuado de protección de la ciberseguridad.

Ello implica la realización de pruebas de simulación de adversarios, el examen de los riesgos a escala y la especial atención a los incidentes graves. Lo que significa la necesidad de supervisión y vigilancia de estos modelos desde el punto de vista de su elaboración y desarrollo, como bajo la perspectiva de su introducción y utilización en el mercado, los incidentes graves que puedan acontecer, así como las medidas correctoras y los niveles correspondientes de seguridad en red.

La cuestión que resulta controvertida es la remisión que hace el párrafo segundo del artículo 55 a los Códigos de buenas prácticas. Y ello porque

20. *Vid*. el artículo 90 del Reglamento de IA relativo a las alertas del grupo de expertos científicos sobre riesgos sistémicos.

prevé la posibilidad de acudir a ellos para demostrar el cumplimiento de estas obligaciones adicionales hasta que se elabore una norma armonizada. En efecto, el artículo 56 del Reglamento de IA relativo a los Códigos de buenas prácticas establece que podrán contener la determinación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión (letra c). Pero, a mayor abundamiento, en su letra d. se refiere a "las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionales a los riesgos y tendrán en cuenta su gravedad y probabilidad y las dificultades específicas para hacerles frente, habida cuenta de la manera en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA".

Lo cierto es que la polémica está servida pues los impulsores del Reglamento de IA han enviado una carta abierta a la Comisaria digital VIKKUNEN, que se ha difundido gracias al *Financial Times*, donde alertan de los peligros de la redacción del Código de buenas prácticas de IA, en relación con los modelos de IA generativa. Concretamente y al hilo de lo expuesto, denuncian la conversión de las obligaciones de evaluación y mitigación de los modelos de IA de uso general con riesgos sistémicos en recomendaciones voluntarias. Teniendo en cuenta que refieren la afección de derechos fundamentales de cientos de millones de personas en la UE. Específicamente, el planteamiento que se denuncia en el Código de Conducta de la Comisión sobre modelos de IA generativa no obligaría a evaluar ni mitigar los riesgos que afecten a derechos fundamentales de los ciudadanos en los riesgos sistémicos, convirtiendo así esta obligación en voluntaria, por la presión que están ejerciendo las grandes plataformas digitales. Asimismo, parece ser que también rebaja determinados requisitos del deber de transparencia. La carta es muy clara cuando alerta de que aceptar tal prerrogativa sería "peligroso, antidemocrático y crea inseguridad jurídica" y continúa señalando que "si los proveedores de los modelos de IA de uso general de mayor impacto adoptaran posiciones políticas más extremas, implementaran políticas que socavaran la fiabilidad del modelo, facilitaran la interferencia extranjera o la manipulación electoral, contribuyeran a la discriminación, restringieran la libertad de información o difundieran contenidos ilegales, las consecuencias podrían perturbar profundamente la economía y la democracia de Europa"[21].

21. *Vid*. "EU Lamakers warn against 'dangerous' moves to water down AI Rules", *Financial Times*, publicado el 25 de marzo de 2025, en https://www.ft.com/content/9051af42 (consultado el 28/4/2025). En efecto, entre los firmantes de la carta se encuentran la mayoría de eurodiputados que impulsaron el Reglamento de IA, incluida la española Carme Artigas que lideró el equipo que elaboró la versión final del Reglamento de IA.

En definitiva, la ausencia de una normativa de desarrollo armonizada que regule esta circunstancia ya ha creado problemas antes de su implementación. El desarrollo de un marco regulador genérico no parece ser la mejor solución cuando se asiste a la enorme presión de las grandes tecnológicas y, parece ser, a los cambios de planteamiento político en la propia Comisión. Y lo grave es situar este planteamiento en un contexto de afección a escala de los derechos fundamentales de cientos de millones de ciudadanos en la UE. La generalidad de este marco regulador no ayuda a la operatividad combinada con el Reglamento de servicios digitales que adolece, asimismo, de falta de concreción en sus prerrogativas, tal y como se expone a continuación. La aplicación de la DSA ya ha generado la apertura de varios procedimientos formales por incumplimiento, a instancia de la Comisión, contra los principales gigantes digitales. Si bien es cierto que los expertos informáticos acusan de obsolescencia a una normativa, incluso antes de su aplicación plena, no lo es menos que la implicación de derechos fundamentales exige una normativa que garantice la protección de los mismos y la seguridad jurídica.

2. LOS RIESGOS SISTÉMICOS EN LA DSA

2.1. Categorías de riesgos sistémicos en la DSA

El modelo de responsabilidad del Reglamento de servicios digitales o la DSA se configura en un sistema de exención con base en una serie de obligaciones asimétricas que se derivan del deber de diligencia debida para los operadores de intermediación en la prestación de servicios digitales, con particular importancia de las plataformas digitales de muy gran tamaño.

De suerte que en el desarrollo de su carácter asimétrico, en primer lugar, se detalla una serie de obligaciones que afectan a todos los intermediarios (arts. 11 a 15). Seguidamente, se establecen otras obligaciones dirigidas a los proveedores de servicios de alojamiento de datos y a las plataformas en línea (arts. 16 a 18) y, a continuación, las obligaciones adicionales para las plataformas en línea (arts. 19 a 32). Finalmente, las disposiciones relativas específicamente a la gestión de riesgos sistémicos se aplican, únicamente, a las plataformas en línea de muy gran tamaño (Sección 5, arts. 33 a 43), aquellas que cuentan con 45 millones de usuarios mensuales activos, que son objeto de análisis de este trabajo.

El diario afirma que el nuevo equipo digital de la Comisión que inició su mandato el pasado diciembre de 2024 quiere centrarse más en atraer inversiones y que quizá ello también explique la retirada de la esperada Directiva de responsabilidad de IA, como un "impulso más amplio para la desregulación" (la traducción es nuestra).

El Reglamento expone con claridad en sus Considerandos las cuatro categorías de riesgos sistémicos que deben evaluar las plataformas y buscadores digitales de muy gran tamaño y que se reproduce a continuación. Así, "(l)a primera categoría se refiere a los riesgos asociados a la difusión de contenidos ilícitos, como la difusión de materiales de abuso sexual de menores o delitos de incitación al odio, u otros tipos de usos indebidos de sus servicios para cometer delitos, y la realización de actividades ilícitas como la venta de productos o servicios prohibidos por el Derecho de la Unión o nacional, incluidos los productos peligrosos o falsificados o el comercio ilegal de animales. Por ejemplo, esa difusión o esas actividades pueden constituir un riesgo sistémico significativo cuando el acceso a contenidos ilícitos pueda propagarse rápida y ampliamente a través de cuentas con un alcance especialmente amplio o de otros medios de amplificación. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben evaluar el riesgo de difusión de contenidos ilícitos, con independencia de que la información sea o no además incompatible con sus condiciones generales. Esta evaluación se entiende sin perjuicio de la responsabilidad personal del destinatario del servicio de plataformas en línea de muy gran tamaño o de los propietarios de sitios web indexados por motores de búsqueda en línea de muy gran tamaño ante la posible ilegalidad de su actividad con arreglo al Derecho aplicable"[22].

"Una segunda categoría se refiere a los efectos reales o previsibles del servicio para el ejercicio de los derechos fundamentales, tal como los protege la Carta, entre ellos, la dignidad humana, la libertad de expresión y de información, incluidos la libertad de los medios de comunicación y su pluralismo, el derecho a la vida privada, el derecho a la protección de datos, el derecho a la no discriminación, los derechos del niño y la protección de los consumidores. Estos riesgos pueden derivarse, por ejemplo, del diseño de los sistemas algorítmicos utilizados por la plataforma en línea de muy gran tamaño o el motor de búsqueda en línea de muy gran tamaño o por el uso indebido de su servicio mediante el envío de notificaciones abusivas u otros métodos destinados a limitar la expresión u obstaculizar la competencia. Al evaluar los riesgos para los derechos del niño, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben tener en cuenta, por ejemplo, cuan fácil les resulta a los menores comprender el diseño y el funcionamiento del servicio, así como la manera en que los menores pueden verse expuestos, a través de su servicio, a contenidos que puedan perjudicar su salud y su desarrollo físico, mental y

22. *Vid.* el Considerando número 80 del Reglamento de Servicios Digitales.

moral. Tales riesgos pueden surgir, por ejemplo, con interfaces en línea que estén diseñadas de manera que exploten intencionada o involuntariamente las debilidades y la inexperiencia de los menores o que puedan generar un comportamiento adictivo"[23].

"Una tercera categoría de riesgos se refiere a los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, así como sobre la seguridad pública"[24].

"Una cuarta categoría de riesgos se deriva de preocupaciones similares relacionadas con el diseño, el funcionamiento o la utilización, también mediante la manipulación, de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño, con un efecto negativo real o previsible en la protección de la salud pública, los menores y graves consecuencias negativas para el bienestar físico y mental de una persona, o en la violencia de género. Estos riesgos también pueden derivarse de campañas coordinadas de desinformación relacionadas con la salud pública, o del diseño de interfaces en línea que puedan estimular adicciones comportamentales de los destinatarios del servicio"[25].

2.2. Evaluación y mitigación de riesgos sistémicos en la DSA

Como se ha señalado con anterioridad, en este punto, el Reglamento de servicios digitales o DSA introduce una serie de obligaciones adicionales que se aplican únicamente a las plataformas digitales de muy gran tamaño (aquellas con más de 45 millones de usuarios mensuales activos). La arquitectura de este sistema tiene su piedra angular en las obligaciones de los arts. 34 y 35, relativas, respectivamente, a la evaluación y mitigación de riesgos. Estas obligaciones adicionales aglutinan diferentes peligros y efectos negativos de los servicios y del análisis de contenidos, en relación directa con los servicios publicitarios que concurren de forma generalizada en estos servicios digitales prestados por las grandes plataformas. En ellas se pretende hacer frente a la difusión de contenido ilícito, su eliminación, así como evitar la vulneración de derechos fundamentales y otros problemas.

A. La evaluación de riesgos sistémicos en la DSA

La evaluación de riesgos sistémicos prevista en el artículo 34 de la DSA prevé la obligación para las plataformas de muy gran tamaño de realizar

23. *Vid.* el Considerando número 81 del Reglamento de Servicios Digitales.
24. *Vid.* el Considerando número 82 del Reglamento de Servicios Digitales.
25. *Vid.* el Considerando número 83 del Reglamento de Servicios Digitales.

anualmente una valoración crítica de sus propios servicios atendiendo a la gravedad y probabilidad de los riesgos. A tal efecto, estos gigantes digitales deben detectar, analizar y evaluar con diligencia los riesgos sistémicos en la UE derivados del funcionamiento o los sistemas de sus servicios, incluidos los algoritmos o del uso que se haga de sus servicios. En particular, se enumeran tres tipos de riesgos sistémicos y loa factores y circunstancias que pueden concurrir. A saber, a. La difusión de contenido ilícito a través de sus servicios, b. Cualquier efecto negativo para el ejercicio de los derechos fundamentales (dignidad humana, vida privada y familiar, protección de datos, libertad de expresión e información (incluidos los medios de comunicación), no discriminación, derechos de menores y de consumidores (arts. 1, 7, 8, 11, 21, 24 y 38 de la Carta Europea), c. Cualquier efecto negativo sobre el discurso cívico y los procesos electorales, la seguridad pública, la violencia de género, la salud pública y los menores y el bienestar físico y psíquico de las personas. A tal efecto, las grandes plataformas tendrán en cuenta la concurrencia de una serie de factores, a saber, el diseño de sus sistemas de recomendación y sus algoritmos, los de moderación de contenidos, las condiciones generales y el uso de los datos[26]. Además, también tendrán que

26. En este sentido, conviene referir lo que el Reglamento de servicios digitales o DSA desarrolla en los Considerandos sobre los sistemas algorítmicos, en concreto, los sistemas de recomendación y publicidad. Concretamente, afirma que "(a)l evaluar dichos riesgos sistémicos, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben centrarse en los sistemas u otros elementos que puedan contribuir a los riesgos, incluidos todos los sistemas algorítmicos que puedan ser pertinentes, en particular sus sistemas de recomendación y de publicidad, dedicando atención a las prácticas conexas de recogida y uso de datos. También deben evaluar si sus condiciones generales y su cumplimiento son adecuados, así como sus procesos de moderación de contenidos, herramientas técnicas y recursos asignados. Al evaluar los riesgos sistémicos identificados en el presente Reglamento, dichos prestadores también deben centrarse en la información que no sea ilícita, pero que contribuya a los riesgos sistémicos identificados en el presente Reglamento. Por consiguiente, dichos prestadores deben dedicar especial atención a cómo se utilizan sus servicios para difundir o amplificar contenidos incorrectos o engañosos, incluida la desinformación. Cuando la amplificación algorítmica de la información contribuya a los riesgos sistémicos, dichos prestadores deben reflejarlo debidamente en sus evaluaciones de riesgos. Cuando los riesgos estén localizados o existan diferencias lingüísticas, dichos prestadores también deben tenerlo en cuenta en sus evaluaciones de riesgos. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben evaluar, en particular, cómo contribuyen a tales riesgos el diseño y el funcionamiento de su servicio, así como la manipulación intencionada y, a menudo, coordinada y el uso de sus servicios, o la infracción sistémica de sus condiciones generales de servicio. Estos riesgos pueden derivarse, por ejemplo, del uso no auténtico del servicio, como la creación de cuentas falsas, el uso de *bots o el uso engañoso de un servicio, y otros comportamientos total o parcialmente*

considerar si estos riesgos se ven influidos por la *manipulación intencionada* de su servicio. Concretamente, por el uso no auténtico o la explotación automatizada del servicio y la difusión de contenido ilícito y de información contraria a sus condiciones generales, eliminando la mención a la publicidad que se realizaba con anterioridad a la versión definitiva[27].

La ausencia de una definición autónoma de "contenido ilícito" en el Reglamento se ha erigido como uno de los problemas más señalados para su aplicación uniforme. La propia Comisión reconoce que el Reglamento de servicios digitales o DSA "no determina si un determinado tipo de contenido puede considerarse ilícito" y que "la ilicitud del contenido viene determinada por las distintas legislaciones nacionales o, en los ámbitos que están armonizados, por la normativa europea". En cuanto al contenido ilícito armonizado para toda la UE, la Comisión refiere específicamente "determinados tipos de contenido ilícito que se presentan y se difunden en línea", en particular, el contenido terrorista y la incitación ilegal al odio (racismo y xenofobia) en línea y con peligro de viralidad. En particular, primero, los delitos de terrorismo y relacionados con grupos o actividades terroristas, así como las medidas para sus víctimas[28]. Y, en segundo lugar, el delito de incitación pública al odio o la violencia contra grupos o personas en relación con la raza, el color o la religión, ascendencia u origen nacional o étnico[29]. Incluyendo, asimismo, la

automatizados, que pueden dar lugar a la difusión rápida y extendida de información al público que sea un contenido ilícito o incompatible con las condiciones generales de una plataforma en línea o un motor de búsqueda en línea y que contribuya a campañas de desinformación". Vid. el Considerando número 84 del Reglamento de Servicios Digitales.

27. En materia de normativa de restricción relativa a la publicidad en línea, *vid.* LAPIEDRA ALCAMÍ, R.M.: "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad" en CASTELLÓ PASTOR, J.J.(Dir.): *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 205-226.

28. *Vid.* la *Recomendación de la Comisión…, cit. supra,* p. 3, párr. 11. En relación con el terrorismo, el Reglamento (UE) 2021/784, del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea especifica que consiste en material que incite al terrorismo, enaltecimiento de actos terroristas, inducción o contribución a la participación en actividades terroristas, instrucciones para la elaboración de armas para actos terroristas o su amenaza. En estos casos, los prestadores tienen la obligación de retirada de dicho contenido en una hora a instancia de los Estados miembros y deben bloquear el acceso a sus servicios cuando se dé tal contenido. *Vid.* DO L 172, de 17 de mayo de 2021.

29. En relación con el Código de conducta para la lucha contra la incitación al odio en línea, la Comisión explica que las plataformas de redes sociales, de muy gran tamaño, se han "comprometido a evaluar y, en caso necesario, suprimir todo contenido de incitación al odio que se les haya notificado, en la mayoría de los casos, en un plazo de 24 horas; el acatamiento de esa norma es supervisado por una red de alertadores

apología, negación o banalización flagrante de genocidios, crímenes contra la humanidad, de guerra o contra la paz, en estos casos[30].

Este contenido armonizado no plantea problemas, con excepción en ámbitos que pueden escapar del tipo, como, por ejemplo, la "banalización flagrante" —ahora digital, con su correspondiente difusión masiva y posible viralización—. En estos casos, la respuesta es mucho más compleja por cuanto, pudiendo atentar contra la libertad de expresión y, además, cada Estado miembro lo regula de forma diversa, con las consecuencias negativas que podría conllevar para la extraterritorialidad de las órdenes de los EEMM contra el contenido ilícito[31]. En este sentido, las verdaderas dificultades se ciernen sobre el contenido ilícito no armonizado por el Derecho de la UE —cuya regulación también puede variar de un Estado miembro a otro— y, también, de los citados "efectos negativos" o contenido nocivo como, por ejemplo, la desinformación. A tal efecto, el Aquí el problema es doble, en el sentido en que, por un lado, será la propia gran plataforma la que decida qué contenidos se consideran como nocivos. Y, por otro, lo harán de forma automatizada a través de algoritmos y modelos generales o sistemas de IA.

Pero, en cualquier caso, la cuestión radica, de nuevo, en la determinación de qué debe considerarse como "cualquier efecto negativo"[32]. A tal efecto,

---

fiables. La Comisión y los signatarios del Código de Conducta lo han revisado en el contexto, entre otras circunstancias, de la entrada en vigor del artículo 45 del Reglamento (UE) 2022/2065, con el fin de introducir compromisos que puedan ayudar a mitigar los riesgos sistémicos y anticipar las amenazas de oleadas de incitación ilegal al odio antes de que ese contenido se haya vuelto viral en línea". *Vid.* la *Recomendación de la Comisión…, cit. supra,* p. 5, párr. 18.

30. *Vid.* la *Recomendación de la Comisión…, cit. supra,* p. 3, párr. 13. En relación con estos delitos, *vid.* la Decisión Marco 2008/913/JAI del Consejo, de 28 de noviembre de 2008, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal, DO L 328, de 6 de diciembre de 2008.

31. Precisamente, en relación con las órdenes de retirada de contenido ilícito que pueden dictar los Estados miembros, la Comisión afirma que el artículo 9 de la DSA "deja claro que tales órdenes pueden emitirse con carácter transfronterizo". *Vid.* la *Recomendación de la Comisión…, cit. supra,* p. 4, párr. 14. Con respecto a la extraterritorialidad del Reglamento de inteligencia artificial, *vid.* BARRIO ANDRÉS, M.: "Consideraciones sobre el ámbito extraterritorial del Reglamento europeo de inteligencia artificial" *Derecho digital e innovación. Digital Law and innovation Review*, núm. 20, 2024 y ORTEGA GIMÉNEZ, A.: "La extraterritorialidad del futuro Reglamento europeo de inteligencia artificial", *Revista Jurídica Colex*, núm. 36, 2024, pp. 22-23.

32. La DSA, en este sentido especifica que "(a)l determinar la importancia de los posibles efectos e impactos negativos, los prestadores deben tener en cuenta la gravedad del impacto potencial y la probabilidad de todos esos riesgos sistémicos. Por ejemplo, podrían evaluar si el potencial impacto negativo puede afectar a un gran número

el art. 34. 1 refiere cualquier efecto negativo, real o previsible, sobre los derechos fundamentales. Y a partir de aquí elabora una lista cerrada pero no exhaustiva de algunos derechos de la Carta europea, a saber, dignidad humana, vida privada y familiar, protección de datos, libertad de expresión e información, no discriminación, derechos de menores y de consumidores (arts. 1, 7, 8, 11, 21, 24 y 38 de la Carta Europea). Lo cierto es que en los párrafos subsiguientes incluyen también la protección de menores o la salud física y mental, obviando otros aspectos como la protección laboral[33] o social o medioambiental[34]. Finalmente, conviene hacer referencia a la "manipulación intencionada" que podría afectar a contenidos legales para su consideración como "nocivos".

Asimismo, conviene señalar otras cuestiones relevantes que relacionan esta circunstancia con el Reglamento de IA. Lo cierto es que la detección de estos riesgos sistémicos a gran escala se realiza a través de sistemas automatizados que podrían inducir a error —por sesgo discriminatorio o error en el resultado— y cuyos diseños y herramientas de desarrollo debieran someterse a control[35]. Asimismo, y aunque excede del objeto de análisis de este trabajo, tampoco puede perderse de vista la cuestión relativa al acceso y tratamiento de datos. Concretamente, por lo que se refiere a las grandes plataformas y el uso masivo de datos personales que conculcan el derecho a la protección de datos personales y a la intimidad y que, sobre todo en determinadas prácticas de publicidad dirigida, concretamente en los anuncios basados en el rastreo, especialmente polémico, se configuran como riesgos sistémicos[36].

---

de personas, su posible irreversibilidad o la dificultad de subsanarlo y restablecer la situación existente antes del impacto potencial". *Vid.* el Considerando número 79 del Reglamento de Servicios Digitales.

33. En este sentido, *vid*. LAPIEDRA ALCAMÍ, R.M.: "La Protección reforzada del trabajador en el Derecho internacional privado europeo: especial referencia a los nómadas digitales", *Actualidad Jurídica iberoamericana*, núm. 20, 2024, pp. 1288-1319.

34. En este sentido, y en el ámbito de las plataformas digitales de gran tamaño y la existencia de colectivos especialmente vulnerables, cabe cuestionarse si no se deberían haber incluido otros derechos de la Carta como por ejemplo los derechos de las personas mayores (art. 26) o la integración de las personas discapacitadas (art. 26). Por no referir otros ámbitos especialmente sensibles como el derecho a la educación (art. 14) o la diversidad cultural (art. 22).

35. *Vid*., por todos, CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional (CDT)*, vol. 17, núm. 1, marzo de 2025, pp. 308-328.

36. En este sentido, los operadores y analistas coinciden en la influencia que han tenido los problemas sistémicos de aplicación de la normativa europea sobre protección de

B. Las medidas de mitigación de riesgos sistémicos de la DSA

Las grandes plataformas digitales tendrán la obligación de adoptar medidas efectivas contra los riesgos sistémicos que hayan detectado según lo previsto en el artículo 34. Estas medidas, además de efectivas, deben ser proporcionadas y adaptarse a los riesgos de manera razonable según el artículo 35. Además, el precepto establece, específicamente, una especial consideración de las consecuencias de los riesgos sistémicos en los derechos fundamentales[37]. Estas medidas se concretan en la adaptación del diseño, características y funcionamiento de sus servicios (incluidas las interfaces en línea), de las condiciones generales y de los aspectos relativos a los procesos de moderación de contenidos. En este sentido, se especifica que se incluye, asimismo, la velocidad y la calidad del tratamiento de las notificaciones de

---

datos en la elaboración del Reglamento de servicios digitales, en particular, y en toda la normativa del paquete digital europeo, en general. *Vid.* BURI, I., VAN HOBOKEN, J.: "The DSA supervision and enforcement architecture", June 24, 2022, *in Analysis*. Básicamente, el Reglamento de Gobernanza europea de datos, en vigor el 24 de septiembre de 2024, pretende fomentar la disponibilidad de datos del sector público para su reutilización en todos los sectores, sobre todo, energía, movilidad y salud, incluyendo la puesta en común de datos entre empresas y su utilización para fines no lucrativos. Por lo que respecta a los datos en el proceso de aplicación del Reglamento, se prevé el acceso, tanto a usuarios, como a investigadores autorizados y organismos civiles. No cabe duda de la necesidad de preservar el deber de confidencialidad de los mismos y la proporcionalidad en la difusión suficiente para acreditar la existencia de una infracción. La evaluación de la existencia de riesgos sistémicos de las grandes plataformas, tanto para la identificación de la infracción o incumplimiento de la normativa, como la adopción de medidas aplicadas para su corrección y subsanación conculcan, desde luego, derechos fundamentales. Y la gestión y designación de estos expertos y auditores, en muchos de los casos, depende de la gestión de las autoridades nacionales competentes y no siempre de la Comisión, lo que requerirá una especial cautela en su desarrollo. *Vid.* BURI, I., VAN HOBOKEN, J.: "La propuesta de…", *op. cit. supra*, p. 20.

37. En este sentido, el Reglamento es muy claro y afirma que "(l)os prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben desplegar los medios necesarios para reducir diligentemente los riesgos sistémicos determinados en las evaluaciones de riesgos, respetando los derechos fundamentales. Cualquier medida que se adopte debe respetar los requisitos de diligencia debida del presente Reglamento y ser eficaz y apropiada para reducir los riesgos sistémicos específicos detectados. Deben ser proporcionadas a la luz de la capacidad económica del prestador de la plataforma en línea de muy gran tamaño o del motor de búsqueda en línea de muy gran tamaño y de la necesidad de evitar restricciones innecesarias al uso de su servicio, teniendo debidamente en cuenta los posibles efectos negativos en dichos derechos fundamentales. Dichos prestadores deben dedicar especial atención al impacto en la libertad de expresión". *Vid.* el Considerando número 79 del Reglamento de Servicios Digitales.

determinados contenidos ilícitos, la retirada de los mismos o el bloqueo a su acceso, especialmente, en lo que refiere a incitación ilegal al odio o la ciberviolencia[38]. Estas medidas también incluyen la adaptación de los algoritmos (incluidos los sistemas de recomendaciones y de los sistemas de publicidad propios y asociados. Además, deberán reforzar los procesos de detección y tienen la obligación de cooperar con otros operadores (alertadores fiables, órganos de resolución extrajudicial), así como con otras plataformas a través de códigos de conducta y protocolos de crisis. También deberán adaptar su interfaz en línea para mejorar la información de los destinatarios del servicio. Finalmente, deben adoptar medidas específicas para la protección de menores (edad, control parental, denuncia y asistencia) y garantizar la distinción de elementos de IA no humanos.

Como puede compararse, la DSA ha dado una especial importancia a la regulación de los riesgos sistémicos en el grueso de la gestión de riesgos de las grandes plataformas digitales. Sin embargo, se trata de un desarrollo que no ha estado exento de críticas. Hay que tener en cuenta que la redacción de los art. 34 y 35, por su generalidad, podría dar lugar a posibles problemas, sobre todo por la capacidad e imparcialidad de llevar a cabo esta tarea de modo eficaz frente a los servicios en línea predominantes. Por otro, también se han señalado los problemas en la apreciación del contenido ilícito, que *a priori*, parece configurarse como una categoría general que será eliminada de forma automatizada a través de procedimientos de notificación y retirada sin un análisis jurídico en mayor profundidad[39].

---

38. Específicamente, en relación con la notificación y la retirada o bloqueo de acceso de contenidos ilícitos, el Considerando 51 de la DSA establece que "(d)ada la necesidad de tener debidamente en cuenta los derechos fundamentales garantizados por la Carta de todas las partes afectadas, toda acción emprendida por un prestador de servicios de alojamiento de datos a raíz de la recepción de una notificación debe estar *estrictamente orientada*, es decir, debe servir para retirar los elementos de información concretos que se consideren contenidos ilícitos o para bloquear el acceso a ellos, sin afectar indebidamente a la *libertad de expresión y de información* de los destinatarios del servicio. Por lo tanto, las notificaciones deben dirigirse, por regla general, a los prestadores de servicios de alojamiento de datos de los que razonablemente quepa esperar que disponen de la capacidad técnica y operativa para actuar contra dichos elementos concretos (…)". En este sentido, *vid.* PALAO MORENO, G.: "Las órdenes de actuación contra contenidos ilícitos en el nuevo Reglamento europeo de servicios digitales" en CASTELLÓ PASTOR, J.J.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, versión digital.

39. De esta suerte, en su día la Comisión señaló en una propuesta de informe la necesidad de que se trate de contenidos manifiestamente ilícitos o declarados como tal según las especificaciones de las órdenes del artículo 9. Asimismo, se ha señalado la problemática del alcance del art. 34 en relación, no solo a su carácter enumerativo (y las

En definitiva, la adopción de medidas por las grandes plataformas para los supuestos de contenidos nocivos introduce elementos de ambigüedad y consecuencias negativas para la libertad de expresión, además de la necesaria consideración de la noción de orden público —sobre todo, interno—. La primera, aquellos contenidos más minoritarios o marginales que siendo lícitos podrían limitarse al ser considerados como negativos. Y la segunda, la relativa a la decisión de las plataformas de limitar en exceso los contenidos por temor a las sanciones[40]. En último término, conviene señalar la problemática relativa a la cuestión de la "manipulación intencionada" de su servicio. En efecto, esta cláusula podría amparar la restricción de contenidos legales que pudieran considerarse nocivos e, incluso, restringir contenidos ante la duda, única y arbitrariamente, para evitar sanciones[41].

2.3. Los procedimientos formales iniciados por la Comisión contra las grandes plataformas por incumplimiento de las obligaciones de la DSA

La implementación de la normativa expuesta se ha iniciado y supone un reto extraordinario. Los grandes operadores han comenzado a modificar

---

consecuencias de evaluación del párrafo segundo), sino en relación, asimismo, con otras disposiciones de la DSA, como, por ejemplo, el acceso a datos del art. 40 (en sus párrafos 4 y 11), que refiere, asimismo, a los riesgos sistémicos. Así como en lo relativo a la responsabilidad del órgano de dirección de estos gigantes digitales (art. 41.5) o en lo relativo a los códigos de conducta (art. 45.1). *Vid.* CORDERO ÁLVAREZ, C.I.: "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro" en CASTELLÓ PASTOR, J.J. (Dir.): *Análisis del reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105.

40. *Vid.* BARATA MIR, J.: "Libertad de expresión, regulación y moderación privada de contenidos", *Teoría y derecho. Revista de pensamiento jurídico*, 2022, núm. 32, pp. 88-107, esp. pp. 99 y 100.

41. Es en relación con el peligro de arbitrariedad y el carácter discriminatorio que se pronuncia la DSA, en el Considerando 47, al establecer que "(a)l definir, aplicar y hacer cumplir esas restricciones, los prestadores de servicios intermediarios deben actuar de manera *no arbitraria y no discriminatoria* y tener en cuenta los derechos e intereses legítimos de los destinatarios del servicio, incluidos los derechos fundamentales amparados por la Carta. Por ejemplo, es preciso que los prestadores de plataformas en línea de muy gran tamaño, en particular, tomen debidamente en consideración la libertad de expresión y de información, incluida la libertad y el pluralismo de los medios de comunicación. Todos los prestadores de servicios intermediarios también deben tener debidamente en cuenta las normas internacionales pertinentes para la protección de los derechos humanos, como los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos" *Vid.* el Considerando número 79 del Reglamento de Servicios Digitales.

algunos aspectos de sus sistemas, si bien la Comisión Europea ha iniciado contra ellas varios procedimientos formales de incumplimiento de la DSA.

En efecto, desde agosto de 2023, estos gigantes digitales han empezado a cambiar sus sistemas e interfaces con la finalidad de mejorar los mecanismos de retirada de contenidos ilícitos y de proteger los derechos fundamentales de millones de usuarios en la UE. Por ejemplo, la *red X* incorpora sistemas de apuntes de los usuarios que permiten a estos realizar las denuncias sobre contenidos ilícitos, de fácil acceso y a golpe de clic en la parte superior derecha de la pantalla. En esta línea, otras plataformas como *Apple, Pinterest, Facebook, Instagram* o *TikTok* también han incorporado herramientas sencillas para la denuncia de estos contenidos por parte de los usuarios, así como han aumentado la información sobre moderación de contenido. Y algo parecido ocurre con las recomendaciones personalizadas para las que algunos de estos operadores —*TikTok, Facebook* e *Instagram*— ofrecen la posibilidad de desactivar el *feed* personalizado en sus plataformas. Con especial referencia a la protección de menores para los que *TikTok* y *YouTube*, además de prohibir los anuncios dirigidos a menores, han establecido sus perfiles automáticamente privados, si bien es un tema especialmente sensible en el que el primer cuestionamiento afecta a la fiabilidad de los mecanismos de verificación de la edad[42].

De hecho, la Comisión Europea tiene abiertos varios procedimientos formales contra las grandes plataformas digitales por incumplimiento de la DSA. Entre ellos, conviene señalar, el procedimiento que abrió contra la *red X* (antes *Twitter*) en el mes de diciembre de 2023 en relación con la gestión de riesgos, la moderación de contenidos, la transparencia publicitaria y el acceso a bases de datos. En este caso, se denunciaba la falta de neutralidad e injerencia en procesos electorales y el discurso cívico. En segundo lugar, la Comisión también inició un procedimiento formal contra *TikTok* en 2024 por incumplimiento de la normativa de la DSA en relación con el riesgo de información en los procesos electorales en Rumanía, por injerencia rusa. Además de protección de menores, transparencia en materia de publicidad y acceso de datos para investigadores. Un par de meses más tarde se iniciaba un segundo procedimiento formal tras el lanzamiento de *TikTok Lite* en Francia y España, sin una realización previa de riesgos que podría promover conductas adictivas. En mayo de 2025, la Comisión emitió unas conclusiones preliminares donde confirmaba el incumplimiento de la DSA por parte de este gran operador, por falta de transparencia en materia de publicidad

42. *Vid.* la página Web oficial de la UE, https://digital-strategy.ec.europa.eu/.es/policies/dsa-impact-platforms (consultado el 15 de mayo de 2025).

que puede suponer un obstáculo para la identificación de interferencias de fraude o manipulación.

Asimismo, la Comisión también ha incoado un procedimiento formal por incumplimiento de la DSA, en mayo de 2024, contra *Meta* (propietario de *Facebook* e *Instagram*) por diferentes posibles infracciones de la normativa, relativas a cómo *Facebook* e *Instagram* abordaron la campaña electoral en las elecciones europeas, y que también afecta a la falta de transparencia en publicidad, difusión de desinformación y la supresión de mecanismos de control en procedimientos electorales sin ofrecer una alternativa adecuada. Debe señalarse que la Comisión Europea ha emitido un aviso a *Meta* para que cumpla las obligaciones de la DSA en la Unión Europea desde que, en 2025, eliminara su sistema de verificación de datos por terceros para Estados Unidos. Además, tampoco puede perderse de vista la actividad de la Comisión en otros procedimientos abiertos contra otros grandes operadores digitales de venta de productos como *Aliexpress* o *Temu* por venta de productos ilegales, falta de protección del consumidor, diseño adictivo de sus sistemas y sistemas de recomendación.

Como puede observarse, es evidente que uno de los mayores peligros se encuentra en la manipulación de los procesos electorales y así lo ha manifestado la propia Comisión con la elaboración de unas directrices dirigidas a las plataformas y motores de búsqueda de muy gran tamaño para la reducción de riesgos sistémicos en los procesos electorales[43]. En este sentido, y tras una enumeración no exhaustiva de medidas, se hace especial referencia a las medidas de reducción de riesgos sistémicos relacionados con la inteligencia artificial generativa. En primer término, se aboga por el refuerzo de los procesos internos, que deben detectar y ofrecer información, análisis y datos para poder elaborar y ponderar las medidas que puedan reducir los riesgos en la búsqueda de información sobre las elecciones (candidatos, programas, campaña o recaudación de fondos). Esto es, presencia y actividad de los políticos en el servicio, examen del uso de la plataforma en las elecciones, número de usuarios en el período electoral y especial atención a las técnicas y procedimientos de desinformación y de manipulación de la información. Y teniendo en cuenta el contexto regional, local y lingüístico en que serán aplicadas estas medidas. Asimismo, estas medidas deben basarse en el Código de Buenas Prácticas en materia de desinformación de la Unión Europea.

43. *Vid.* FERNÁNDEZ, C.B.: "La Comisión emite unas directrices dirigidas a las plataformas y motores de búsqueda en línea de muy gran tamaño, para la reducción de los riesgos sistémicos en los procesos electorales", *Diario la Ley, laleynext.e*s, 26 de abril de 2024 (consultado el 15 de abril de 2025).

Específicamente, la Comisión recomienda unas medidas concretas para evitar los riesgos sistémicos en los procesos electorales. A saber, facilitar el acceso a la información oficial sobre el proceso electoral, implementar iniciativas de alfabetización mediática, controlar los sistemas de recomendación para evitar la desinformación y la afección de la opinión pública, favorecer la transparencia de la información política, desmonetización de los contenidos de desinformación. Ello afecta especialmente al uso de la IA generativa —especialmente, *deepfakes* y *bots*— que deberán etiquetarse de manera eficaz para su identificación automática por la plataforma —e individual por el usuario— para evitar que sean sesgados, engañosos o falsos o puedan inducir a error. Deberá indicarse el período temporal de aplicación de estas medidas y realizar una revisión post electoral de su eficacia e incidencia en las elecciones, con medidas específicas para las elecciones europeas.

El enfoque establece una especial atención en la posible vulneración de derechos fundamentales, tanto por lo que respecta a la actuación de la Comisión europea, como por lo que afecta a los grandes operadores digitales. En este sentido, el texto programático de la DSA es claro al afirmar que la Comisión, en estos procedimientos, deberá actuar "respetando plenamente el derecho fundamental a ser oído y a tener acceso al expediente en el contexto de los procedimientos de ejecución, el principio de proporcionalidad y los derechos y los intereses de los afectados"[44]. Del mismo modo y por lo que respecta a los prestadores de las plataformas en línea de muy gran tamaño, así como terceros afectados por una decisión de la Comisión deben tener la oportunidad de presentar sus observaciones de antemano y las decisiones deben revestir la necesaria difusión para su conocimiento. Se garantizan expresamente los derechos de defensa de las partes afectadas y, específicamente, el derecho de acceso al expediente, así como el deber de confidencialidad de la información, en equilibrio con el acceso al contenido de la decisión por parte del justiciable, en relación, tanto con los hechos, como con la motivación de la misma[45].

Asimismo, debe considerarse que la Comisión también debe velar para que los Estados miembros implementen las medidas establecidas en la DSA. El hecho es que, con carácter reciente, la Comisión Europea ha anunciado que demandará ante el TJUE a cinco Estados miembros, entre los que se encuentra España, además de Chequia, Chipre, Polonia y Portugal por infringir la DSA. Concretamente, Polonia no ha designado el

44. *Vid.* el Considerando número 140 del Reglamento de Servicios Digitales.
45. *Vid.* el Considerando número 146 del Reglamento de Servicios Digitales.

coordinador nacional de servicios digitales, que cumple una función clave específicamente en la fase previa a los procesos electorales que, además, tiene convocados este país, bajo el peligro de interferencia y difusión de desinformación de Rusia en las elecciones presidenciales. Y ello porque estos entes organizan encuentros y pruebas de resistencia con las grandes plataformas para ponderar las amenazas de desinformación en línea que podrían afectar al proceso electoral, y que habían concurrido en las pasadas elecciones de Alemania y Rumanía. Por su parte, Chequia, Chipre y Portugal, aunque sí que han designado un coordinador nacional, no le han atribuido competencias para llevar a cabo su labor, así como tampoco han establecido sanciones por incumplimiento de la DSA. Pese a las cartas de emplazamiento y dictámenes motivados enviados por la Comisión Europea a estos cinco Estados miembros, estos no han adoptado las medidas necesarias en aplicación de la DSA. Será pues el TJUE el que determine si se ha producido la infracción, si bien la Comisión Europea puede solicitar la imposición de sanciones durante el procedimiento[46].

Parece que la ofensiva de la Comisión se intensifica por cuanto, con carácter reciente, ha realizado una acusación formal contra plataformas de muy gran tamaño, por incumplimiento de otro instrumento regulador que es el Reglamento de mercados digitales (DMA), a las que ha enviado conclusiones preliminares[47]. Así, se ha dirigido contra *Alphabet* (propietaria de *Google*), por favorecer de manera sistemática sus propios servicios, como son *Google Shopping*, *Google Hotel*s y *Google Flights*, incorporándolos de manera preferencial en sus motores de búsqueda y alterando de forma anticompetitiva los resultados de las mismas. Asimismo, también se ha señalado que *Google* impone restricciones a los desarrolladores de aplicaciones que impiden que los usuarios se puedan dirigir a ofertas externas a su propia *Play Store*. Además, la Comisión también investiga a *Google* para dilucidar si la implementación de del sistema de IA *Overviews* —conocida como "vistas creadas con IA"— para la generación de resúmenes por inteligencia artificial, vulnera la DMA, además de la normativa de protección de los derechos de autor. Y lo mismo ocurre con *Apple* a quien la Comisión Europea ha solicitado la apertura de sus sistemas operativos con el objeto de mejorar la interoperabilidad con otros operadores, mejorando la competencia y las opciones de los usuarios.

---

46. *Vid. Euractiv*.es, de 7 de mayo de 2025, en https://euractiv.es/section/all/news/commission-takes-four-eu-countries-to-court-over-digital-services-law-failures/.
47. *Vid*. https://ec.europa.eu/commission/presscorner/detail/es/ip_25_811 (consultado el 15 de mayo de 2025).

3. LA APLICACIÓN CONJUNTA DE AMBOS REGLAMENTOS

El texto del Reglamento de IA, y en general y como veremos, de la normativa digital y las recomendaciones posteriores de la Comisión, es claro con respecto a la relación de *complementariedad* entre las disposiciones del Reglamento de IA y el Reglamento de servicios digitales por lo que respecta a la gestión de riesgos sistémicos de los modelos de IA de uso general integrados en los servicios de intermediarios de las grandes plataformas digitales. Tal es así, que incluso se afirma que los sistemas de IA sujetos al Reglamento de IA pueden presentarse como servicios intermediarios o partes de estos en el sentido del Reglamento de servicios digitales[48]. Y no solo en términos de responsabilidad donde el artículo 2.5 del Reglamento de IA establece que este último "no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios de intermediación" del Capítulo II del Reglamento de servicios digitales[49].

La parte programática del Reglamento de IA afirma su relación de complementariedad, concretamente en el Considerando 118, y aclara que las obligaciones impuestas a los operadores que introduzcan en el mercado provean o utilicen estos modelos de IA *complementan* las obligaciones de los prestadores de servicios intermediarios que integren dichos modelos en sus servicios del Reglamento de servicios digitales. El Texto precisa que en la medida en que dichos modelos estén integrados en plataformas o buscadores de muy gran tamaño, están sujetos al marco de gestión de riesgos del Reglamento de servicios digitales. Y continúa estableciendo que, en estos casos, se presume el cumplimiento de las obligaciones a no ser que surjan riesgos sistémicos no cubiertos por el Reglamento de servicios digitales y se detecten en estos modelos de IA de uso general, que estarán obligados a evaluar y mitigar conforme al Reglamento de IA.

Lo cierto es que, más allá de una relación de complementariedad, la intencionalidad de la norma da un paso más allá estableciendo que para la evaluación y mitigación de riesgos sistémicos derivados de la difusión de contenidos manipulados artificialmente o de la desinformación. Así, las obligaciones del Reglamento de IA resultan en estos casos "especialmente pertinentes para la aplicación efectiva" del Reglamento de servicios digitales. Esto es, el riesgo de los efectos negativos reales o razonablemente previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, tal y como se expone en el Considerando núm. 120 del Reglamento de IA[50].

48. *Vid.* el Considerando número 119 del Reglamento de Servicios Digitales.
49. En este sentido, *vid*. CORDERO ÁLVAREZ, C.I.: "Inteligencia Artificial y…", *cit. supra*, p. 70.
50. En relación con la exigencia de etiquetar los contenidos generados por IA con arreglo al Reglamento de IA que se entiende sin perjuicio de la aplicación de la obligación

Con posterioridad, la Comisión ha establecido más nexos de unión entre uno y otro instrumento. De suerte que, en relación con la aprobación del *Proyecto de Guía sobre prácticas prohibidas de IA establecidas en el Reglamento de IA*, afirma que el Reglamento de IA se aplica "en conjunto" (*in conjuntion*) con las obligaciones relevantes para proveedores de servicios intermediarios que han integrado modelos de IA del Reglamento de servicios digitales (párrafo 48). En esta misma Comunicación, la Comisión establece otro ejemplo de complementariedad entre ambos instrumentos. Concretamente, señala la prohibición de patrones oscuros (*dark patterns*) del artículo 25.1 del Reglamento de servicios digitales como un ejemplo ("shoud be understood to constitute an example") de las practicas prohibidas del artículo 5.1.a y b del Reglamento de IA, como técnica manipulativa cuando causen daños significativos (párrafo 139)[51].

Razones que nos llevan a interpretar en sentido complementario y de sinergia la interacción en la aplicación del Reglamento de IA y el de servicios digitales en general y, particularmente, en relación con la cuestión relativa a la evaluación y mitigación de riesgos sistémicos de los grandes proveedores de servicios intermediarios que han integrados modelos de IA de uso general en sus servicios.

III. CONCLUSIONES

La incorporación de modelos generales de IA en los servicios de intermediación de las grandes plataformas digitales ha elevado exponencialmente lo que se ha dado en llamar la *algoritmización* de la sociedad. Un salto —bajo lógica de reemplazo y en palabras de INNERARITY— de humanos que renuncian a tomar decisiones y máquinas capaces de hacerlo que implica un *rediseño institucional de la sociedad*[52].

Las grandes plataformas incorporan modelos generales de inteligencia artificial para el tratamiento y difusión de contenidos, tanto para la adopción

---

del artículo 26.6 del Reglamento de servicios digitales. Obligación relativa a los prestadores de servicios de alojamiento de datos de tratar las notificaciones que reciban sobre contenidos ilícitos en virtud del artículo 16.1 de dicho Reglamento, que no debe influir en la evaluación y la decisión sobre el carácter ilícito del contenido que se trate. Dicha evaluación debe realizarse únicamente con referencia a las normas que rigen la legalidad del contenido. *Vid*. Considerando 136 del Reglamento de IA.

51. *Vid*. El *Annex to the Communication to the Commission: Approval of the content of the draft Communication fron the Commission — Commission Guidelines on prohibited artificial intelligence practices by Regulation (EU) 2024/1689 (AI Act)*, Bruselas, 4 de febrero de 2025, C (2025) 884 final, Annex, esp. párrs. 48 y 139.

52. *Vid*. INNERARITY, D.: *Una teoría crítica de la inteligencia artificial*, Madrid, Galaxia Gutenberg, 2025. 552 pp.

automatizada de decisiones, como para la verificación de contenidos, con sistemas algorítmicos de moderación de contenidos y de curación o recomendación, incluida la publicidad. Asimismo, también se utilizan los sistemas de inteligencia artificial generativa para la elaboración de contenidos que se publican y difunden por los servicios en línea de estos grandes operadores digitales. Estos contenidos pueden resultar ilícitos o producir información no deseada o manipulación de la misma que dé lugar a desinformación. Cuando estos problemas afectan a derechos fundamentales o a la sociedad en su conjunto pueden clasificarse como riesgos sistémicos. Estos se regulan con base en el establecimiento de una serie de obligaciones adicionales, tanto en el Reglamento de inteligencia artificial, como en el Reglamento sobre servicios digitales en régimen de aplicación combinada y complementaria.

En este contexto, la elaboración de un marco regulador para la creación de un entorno digital seguro y justo en la UE resulta ser un desafío de enorme complejidad. La UE ha decidido, ya que no es líder tecnológico, emprender el desarrollo de una normativa digital pionera y rigorosa que, probablemente, podría exportarse bajo el denominado *efecto Bruselas*, con todas las consecuencias mejores y peores que ello implica (qué ocurriría si esta normativa fuese incorporada en países con déficit democrático o claramente autoritarios, lo que se conoce como el *test Putin*).

Sin embargo, los obstáculos que surgen tienen difícil solución. La presión de las grandes plataformas digitales que imperan en el mercado y que defienden sus propios intereses —comerciales— unido al carácter político de la Comisión a la hora de abordar estos retos, convergen con la eventual vulneración masiva de los derechos fundamentales y las libertades públicas de cientos de millones de ciudadanos en la UE. Y ello porque la incorporación de los modelos de IA de uso general, tanto en la moderación y curación de contenidos, como para su generación por las grandes plataformas digitales elevan exponencialmente el gran impacto y alcance de los resultados negativos. Como, por ejemplo, la desinformación, la censura, la vulneración de la libertad de expresión o la afección de procesos electorales y derechos, a ciudades enteras, comunidades o colectivos.

A tal efecto, se establecen unas obligaciones adicionales de riesgos sistémicos que deben cumplir las grandes plataformas con respecto a los modelos de IA de uso general integrados en sus servicios digitales. Estas obligaciones adicionales se prevén, tanto en el reglamento de IA, como en el Reglamento de servicios digitales y su aplicación y operatividad, tal y como se ha expuesto, son complementarias. Es más, por lo que se refiere a

riesgos sistémicos de IA, las disposiciones del Reglamento de IA se presentan como "especialmente pertinentes para facilitar la aplicación efectiva" de la DSA. Estas obligaciones adicionales imponen a las grandes plataformas evaluar y gestionar los riesgos sistémicos de sus servicios digitales a través de diferentes acciones. Entre ellas, prevenir las actividades ilícitas y nocivas en línea y la difusión de desinformación, así como garantizar la seguridad y los derechos fundamentales de los usuarios, con la obligación de información y transparencia y bajo la obligación general de la diligencia debida.

No obstante, los problemas no se localizan tanto en la conjunción de ambos instrumentos normativos sino en su propia implementación. Por un lado, la Comisión ya tiene abiertos varios procedimientos formales por incumplimiento de la DSA a varias grandes plataformas digitales (*X, TikTok y Meta*, entre otras) donde se ha señalado que el ámbito de vulnerabilidad y riesgo sistémico común es la injerencia y desinformación en los procesos electorales y, por ende, la manipulación del discurso cívico. Y, por otro lado, las dificultades derivadas del enorme poder e influencia de las grandes plataformas digitales en la propia implementación y desarrollo de la normativa. El hecho es que la elaboración del actual Código de conducta de IA amenaza con rebajar las exigencias del Reglamento de IA. En efecto, se han levantados voces autorizadas que alertan de la eliminación del carácter vinculante de la evaluación y mitigación de riesgos sistémicos que afectan a derechos fundamentales de los ciudadanos, debido a las presiones de estos grandes operadores digitales.

Lo cierto es que resulta muy difícil eludir el poder de los pocos gigantes digitales que controlan el espacio digital, que ha derivado hacia lo que algunos autores denominan como *tecnofeudalismo* o, incluso, *tecnofascismo*. En efecto, no parece razonable dejar en manos de entes privados la determinación de qué es un contenido ilícito o cuándo se producen efectos negativos sobre los derechos fundamentales o la sociedad en su conjunto y la adopción de medidas restrictivas y mitigadoras de los riesgos sistémicos, en otras palabras, el poder del control del tratamiento y la difusión de contenidos. Esto es, la potestad de decidir si esos contenidos son aceptables o no, su posible manipulación y su retirada de internet, lo que puede derivar en desinformación, censura y atentar contra la libertad de expresión. Como se ha visto, la práctica demuestra que el sistema, tal y como se articula en el marco normativo de la Unión europea, resulta ineficaz para la consecución de un entorno digital justo y seguro. Tampoco el control estatal resulta del todo apropiado cuando se piensa en la incorporación del modelo en ordenamientos jurídicos con déficit democrático o autoritarios —cada vez más

cercanos— y en un contexto de diversidad normativa en el que, además, cada Estado miembro regula de forma distinta la consideración de contenidos ilícitos o nocivos.

La dificultad radica en hallar un equilibrio entre el control y los beneficios de la IA, sobre todo, porque refiere a control de riesgos y garantías que afectan a derechos humanos. No cabe duda de que la legislación tiene que adaptarse de forma proactiva al avance tecnológico de la IA y estar especialmente alerta a la calidad democrática de los medios utilizados en su empeño, siempre bajo un eventual control judicial. Sin embargo, se trata de una labor que requiere una especial cohesión social para llevarse a cabo. Un desafío que implica la colaboración necesaria de todos los operadores implicados: sistemas de control públicos y privados, la acción coordinada de Estados y grandes entes privados digitales y, en definitiva, de toda la sociedad civil.

BIBLIOGRAFÍA

BARATA MIR, J.: "Libertad de expresión, regulación y moderación privada de contenidos", *Teoría y derecho: revista de pensamiento jurídico*, 2022, núm. 32, pp. 88-107.

BARRIO ANDRÉS, M.: "Consideraciones sobre el ámbito extraterritorial del Reglamento europeo de inteligencia artificial" *Derecho digital e innovación. Digital Law and innovation Review*, núm. 20, 2024.

BARRIO ANDRÉS, M.: "El efecto Bruselas del Reglamento europeo de inteligencia artificial", *Otrosí, Revista de Colegio de abogados de Madrid*, núm. 2. 2024, pp. 47-48.

BRADFORD, A.: "The European Union in a globalized world: 'The Brussels Effect'", *Revue Européenne du Droit*, 75, 2, marzo de 2021.

BROADVENT, M.: "The Digital Services Act, the Digital Market act, and the New Competion Tool", *Center for Strategic and International Studies*, nov. (2020), publicado en https://apo.org.au/node/309351.

BURI, I., VAN HOBOKEN, J.: "La propuesta de Ley de Servicios digitales (DSA): una visión crítica", DSA Observatory, Instituto de Derecho de la Información (IVIR), Universidad de Ámsterdam, Documento de debate, octubre de 2021, 80 pp.

BURI, I., VAN HOBOKEN, J.: "The DSA supervision and enforcement architecture", June 24, 2022, *in Analysis*.

CASTELLÓ PASTOR, J.J.: "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", *Cuadernos de Derecho Transnacional (CDT)*, vol. 17, núm. 1, marzo de 2025, pp. 308-328.

CASTELLÓ PASTOR, J.J.(Dir.): "Análisis del Reglamento (UE) y su interrelación con otras normas de la Unión europea", Aranzadi, 2024.

CASTELLÓ PASTOR, J,.J.: "Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (p2b): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea" en CASTELLÓ PASTOR, J.J. (Dir.): Análisis del Reglamento de servicios digitales y su interrelación con otras normas de la Unión Europea, Aranzadi, 2024, versión digital.

CASTELLÓ PASTOR, J.J., "Disponibilidad de productos y servicios en línea en el mercado único digital", en CASTELLÓ PASTOR, J. J., GUERRERO PÉREZ, A., MARÍNEZ PÉREZ, M., *Derecho de la contratación electrónica y comercio electrónico en la Unión Europea y en España*, Tirant lo Blanch, Valencia, 2021, pp. 315-352.

CHANDER, A.: "When the Digital Services Act Goes Global", *Berkeley Technology Law Review*, 2023, 19 pp.

CORDERO ÁLVAREZ, C.I.: "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro" en CASTELLÓ PASTOR, J.J. (Dir.): *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105.

DE MIGUEL ASENSIO, P. A.: *Manual de Derecho de las nuevas tecnologías*, Pamplona, Aranzadi, 2023.

DE MIGUEL ASENSIO, P. A.: *Derecho privado de internet*, 6.ª edición, Civitas Thomson-Reuters, 2022.

DE MIGUEL ASENSIO, P. A.: "Propuesta de Reglamento sobre inteligencia artificial", *La Ley Unión Europea*, número 92, 2021.

DE MIGUEL ASENSIO, P. A., "Servicios y mercados digitales: modernización del régimen de responsabilidad y nuevas obligaciones de intermediarios", *La Ley Unión Europea*, núm. 88, enero (2021), 18 pp.

FELIU ÁLVAREZ SOTOMAYOR, S.: "Ámbito territorial y aplicación del principio de control en origen en el Reglamento UE de servicios digitales" en

CASTELLÓ PASTOR, J.J.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 41-64.

FERNÁNDEZ, C.B.: "La Comisión emite unas directrices dirigidas a las plataformas y motores de búsqueda en línea de muy gran tamaño, para la reducción de los riesgos sistémicos en los procesos electorales", *Diario la Ley, laleynext.e*s, 26 de abril de 2024 (consultado el 15 de abril de 2025).

GRAFANAKI, S., "Platforms, the First Amendment and Online Speech: Regulating the Filters", *Pace Law Review*, volume 39 (2018).

HOLT, D. y HAMMEKE, F., *Two-Sided Markets, Platforms and Network Effects, E-Commerce Competition Enforcement Guide*, 2.ª ed., 2019.

INNERARITY, D.: *Una teoría crítica de la inteligencia artificial*, Madrid, Galaxia Gutenberg, 2025. 552 pp.

JIMÉNEZ HORWITH, M., "Las responsabilidades de las plataformas en línea en el ámbito del derecho de los contratos: desde la protección de los consumidores hasta la protección de los profesionales y empresarios. Breves reflexiones sobre el Reglamento (UE) 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea", *Publicaciones Jurídicas. Centro de Estudios de Consumo CESCO* (2020).

KAUSHAL, R., VAN DER KERKHOF, C., GOANTA, C., SPANAKIS, G. Y IAMNITCHI, A.: "Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database", 2024, en https://doi.org/10.48550/arXiv.2404.02894.

LAPIEDRA ALCAMÍ, R.M.: "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad" en CASTELLÓ PASTOR, J.J. (Dir.): *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 205-226.

LAPIEDRA ALCAMÍ, R.M.: "La Protección reforzada del trabajador en el Derecho internacional privado europeo: especial referencia a los nómadas digitales" en Actualidad Jurídica iberoamericana, núm. 20, 2024, pp. 1288-1319.

LAPIEDRA ALCAMÍ, R., "Hacia la transparencia y la equidad en el *ranking* de resultados a la luz del Reglamento 2019/1150" en CASTELLÓ

PASTOR, J.J. (Dir.): *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi (Thomson Reuters), 2021, pp. 161-193.

LLANO ALONSO, F.: *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Valencia, Tirant lo Blanch, 2024.

ORTEGA GIMÉNEZ, A.: "La extraterritorialidad del futuro Reglamento europeo de inteligencia artificial", *Revista Jurídica Colex*, núm. 36, 2024, pp. 22-23.

PALAO MORENO, G.: "Las órdenes de actuación contra contenidos ilícitos en el nuevo Reglamento europeo de servicios digitales" en CASTELLÓ PASTOR, J.J.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, versión digital.

WILMAN, F.: "The Digital Services Act (DSA): An Overview", *SSRN, Comisión Europea*, diciembre 2022, en http://ssrn.com/abstract_4304586 (consultado 15 de abril de 2025).

Capítulo 8

Inteligencia artificial y riesgos sistémicos en la red: la lucha contra la desinformación en la Unión Europea*

Clara Isabel Cordero Álvarez
Prof.ª Contratada Dra. de Derecho Internacional Privado
(Acr. TitularUniversidad Complutense de Madrid (UCM)
Miembro del IDEIR

SUMARIO: I. PLANTEAMIENTO. II. MARCO JURÍDICO EUROPEO FRENTE A LOS RIESGOS DEL USO DE LA IA. 1. *El Reglamento de IA: sistemas de IA para la desinformación ¿sistemas prohibidos, alto riesgo o riesgo moderado?* 2. *Directivas sobre responsabilidad en materia de IA*. 2.1. La Directiva de 2024 sobre productos defectuosos y su posible aplicación al caso. 2.2. Propuesta de Directiva de adaptación de las normas de responsabilidad extracontractual a la IA: oportunidad perdida. 3. *El uso de la IA para la creación de contenidos en la DSA*. III. MECANISMOS DE LUCHA CONTRA LA DESINFORMACIÓN DENTRO DE LA UE EN EL USO DE LOS SERVICIOS DIGITALES. 1. *Obligaciones sustantivas para los grandes prestadores de la DSA y el recurso a la IA para su cumplimiento*. 1.1. La desinformación como riesgo sistémico para grandes plataformas y motores de búsqueda. 1.2. Moderación (proactiva) contra contenidos no deseados: en particular los mecanismos automatizados. 1.3. Curación (recomendación) de contenidos automatizada: peligros en presencia y oportunidades. 2. *La Comisión europea en la lucha contra la desinformación en las redes*. 2.1. Investigaciones en curso frente a muy grandes

* Este trabajo se ha realizado en el marco del Proyecto de Investigación "Hacia una transición digital centrada en la persona en la Unión Europea", TED2021-129307A-I00, financiado por MICIU /AEI/10.13039/501100011033 y por la Unión Europea "NextGenerationEU"/PRTR, de cuyo equipo de investigación es miembro la autora.

plataformas para mitigar riesgos en procesos electorales y discursos cívicos: los casos de TikTok, X y Meta. 2.2. Normas de autorregulación de las plataforma para hacer frente a la desinformación. IV. CONCLUSIONES. BIBLIOGRAFÍA.

I. PLANTEAMIENTO

1. Es indudable que la Inteligencia Artificial (IA) ha transformado radicalmente la forma de interactuar con la tecnología, y la presentación de contenidos no es una excepción. En el contexto digital actual el contenido es esencial y la IA se ha convertido en una herramienta especialmente interesante para su difusión. El presente estudio trata de abordar, dentro de las complejas y aun indeterminadas cuestiones vinculadas al uso de la IA, aquellas relativas a su intermediación en el tratamiento de datos o generación de contenidos y sus consecuencias jurídicas, concretamente en los supuestos de desinformación a través de las muy grandes plataformas digitales —incluidos motores de búsqueda—, como medio global de difusión. El estudio planteado se realizará desde la perspectiva del Derecho de la Unión Europea (UE).

En este contexto, el recurso a la IA (incluida la generativa)[1] puede verse desde una doble aproximación o perspectiva. Por un lado, cabe referir su utilización —especialmente a través de sistemas algorítmicos— cada vez más generalizada por parte de los grandes prestadores de servicios digitales de intermediación dentro de la UE, para el ejercicio de la función de control (moderación proactiva) y de curación o recomendación de contenidos publicados o difundidos a través de sus servicios, en el cumplimiento de las obligaciones impuestas por la normativa europea Por otro lado, el creciente recurso a distinta IA generativa para creación de contenidos atractivos, tanto textos como imágenes y material audiovisual, con información que no está necesariamente verificada —por ejemplo a través de *apps* de IA conocidas como *deepfakes*[2]— cuyo resultado se disemina globalmente a través de las

1. O más ampliamente, de modelos fundacionales, como un tipo de IA generativa: entendido como modelos de gran tamaño de IA entrenados en una gran cantidad de datos no etiquetados a escala que da como resultado un modelo que se puede adaptar a una amplia gama de tareas posteriores. Entre los modelos fundacionales se encuentran Chat GPT-4 de OpenAI, Gemini de Google, Llama 2 de Meta y Claude de Anthropic.
2. Se refiere a una subcategoría de una realidad que ya tiene una denominación propia "*deepfakes*", cada vez más generalizada desde que extendió el fenómeno de las apps de IA. El término *deepfakes* designa imágenes y vídeos modificados por redes neuronales que han pasado por un proceso llamado "aprendizaje automático". Básicamente consiste en que una IA puede cambiar cómo se ve una foto o un video. Los «*deepfakes*"

distintas redes sociales con distintos intereses y sin identificar en muchas ocasiones su origen artificial. Este fenómeno se configurar otro elemento que perfila el nuevo marco de actuación de esta tecnología que requiere de intervención normativa para prevenir y reglamentar indeseados comportamientos y resultados —entre los que se encuentra la desinformación—. A mayor abundamiento, esta difusión de contenidos no reales creados por IA se llega a realizar incluso a través de perfiles que pueden no ser de personas reales, por ejemplo, a través de *bots*[3] o influencers virtuales creados por IA. Los *bots* de redes sociales (o *bots* sociales) son aquellos que generan distinto tipo de actividad no real en estas plataformas en línea; actividades tales como la creación de cuentas de personas ficticias (perfiles falsos), crear seguidores inexistentes, poner "me gusta" a determinados comentarios, publicar comentarios falsos en distintos perfiles (*fake news*), etc. Estos *bots* imitan la actividad humana en las plataformas de las redes sociales persiguiendo distintos objetivos (en función de lo que desee el usuario de este tipo de aplicación), entre otros, enviar *spam* a los contenidos, aumentar la popularidad de un cierto perfil o, en nuestro caso, difundir información falsa o manipulada con la finalidad de desinformar en un determinado sector, materia o contexto (como puede ser típicamente en el marco de un proceso electoral).

2. El punto de partida o presupuesto para el análisis propuesto en este trabajo es la utilización de los servicios digitales de intermediación de las grandes plataformas por los usuarios para publicar y difundir contenidos que contribuyen a la desinformación generados a través de la IA; pero también como resultado —indeseado— de la moderación de contenidos realizado por la propia plataforma digital (así como en la labor de curación) mediante sistemas de IA.

El análisis de las posibles respuestas normativas y la búsqueda de la deseada seguridad jurídica frente a un uso inadecuado de la IA en este ámbito requiere, no sólo del recurso a los instrumentos específicos de regulación del uso de la IA dentro de la UE, sino también —y de manera especial— de

---

más conocidos son los que toman la cara de una persona famosa y la ponen en otro cuerpo, típicamente sin su consentimiento, realizando comportamientos o haciendo manifestaciones que no se corresponde con la realidad, con distintos fines.

3. Un *bot* es una aplicación de *software* automatizada que realiza tareas repetitivas en una red (en este caso, en plataformas de digitales de redes sociales). Dicha aplicación sigue instrucciones específicas para imitar el comportamiento humano, pero es más rápida y precisa, y se puede ejecutar de forma independiente sin intervención humana. A modo de ejemplo, los *bots* pueden interactuar con sitios web, hablar con visitantes/usuarios del sitio o analizar contenidos.

la reglamentación de los servicios digitales (de intermediación) dirigidos al mercado interior, en particular el Reglamento o Ley de servicios digitales (DSA)[4]; ya que de su cumplimiento dependerá la eventual responsabilidad de los prestadores de servicios en línea en estos casos. Con la DSA se establece un marco jurídico de exención condicionada de responsabilidad de los actores digitales de intermediación cubiertos[5], que se encuentra necesariamente vinculado al cumplimiento de un conjunto armonizado de obligaciones sustantivas asimétricas en función de la naturaleza de los obligados (relativas a la diligencia debida). Son de especial relevancia las disposiciones dirigidas específicamente a las plataformas en línea y a los motores de búsqueda de muy gran tamaño para evaluar y gestionar los riesgos sistémicos vinculados a sus servicios digitales; esto es, prevenir las actividades ilícitas y nocivas en línea y la difusión de desinformación, garantizar la seguridad de los usuarios, proteger los derechos fundamentales y consolidar, en definitiva, un entorno digital más justo y abierto[6]. La desinformación, por tanto, se configura como un riesgo sistémico que las grandes plataformas digitales y motores de búsqueda que operan dentro de la UE deben necesariamente evaluar y mitigar. En este ámbito, resulta significativo las nuevas obligaciones de transparencia y rendición de cuentas para estos operadores sobre sus prácticas de moderación y curación de contenidos, esto es, los mecanismos utilizados para detectar, restringir y eliminar contenidos ilícitos o contrarios a sus condiciones generales (como sería típicamente el caso de la desinformación). Entre estos mecanismos se encuentran típicamente, y en un alto porcentaje, los sistemas automatizados con recurso a la IA para la toma de decisiones; lo que no está exento de problemas conectados a los algoritmos utilizados, como son los posibles sesgos y errores en los resul-

4. Digital Services Act (en adelante, DSA). Reglamento (UE) 2022/2065 del Parlamento europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales, DOUE núm. 277, de 27 de octubre de 2022.

5. En general sobre esta cuestión, J.J. CASTELLÓ PASTOR, "Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales", en AA.VV.: *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi Thomson-Reuters, 2021, pp. 37-76; C.I CORDERO ÁLVAREZ, "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro", en AA.VV.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2024, pp. 69-105; A. GASCÓN MARCÉN, "La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro", en AA.VV.: *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2021, pp. 133-160.

6. De conformidad con el art. 1 DSA.

tados. La labor de control y curación de contenidos, con el objeto de luchar contra los riesgos sistémicos y evitar responsabilidades por estos prestadores de servicios, limita libertades fundamentales de los usuarios como es la libertad de expresión[7], por lo que los elementos y factores utilizados con este fin deben adecuados y, en todo caso, objeto de control, en la medida que puedan contribuir incluso a la generación de ese riesgo (la desinformación). Veremos si esto es posible y cómo debería aproximarse esta cuestión.

Se deja al margen del estudio particular del Reglamento sobre la transparencia y la segmentación de la publicidad política[8], presentado como complemento a la DSA, en cuanto a las plataformas digitales de intermediación en relación con la información de *targeting* político difundida a través de sus servicios, como otro instrumento para tratar de salvaguardar los derechos de los usuarios.

3. Las regulaciones sobre IA (directa e indirecta) deben tener especial cuidado en cuanto a la reglamentación del uso de este tipo de tecnología en estos ámbitos. La actual respuesta regulatoria de la UE (así como las iniciativas supranacionales que se van manifestando[9]) pueden parecer poco adecuadas

7. La moderación de contenido algorítmica suele buscar optimizar un único objetivo, como eliminar materiales que infringen derechos de autor o bloquear el discurso de odio, mientras que otros valores de interés público, como el uso justo o la libertad de expresión, suelen descuidarse. Para poder mitigar este peligro se propone la introducción de lo que se denominan algoritmos de impugnación que "introducen un diseño adversarial que refleja valores en conflicto y, por lo tanto, pueden ofrecer un control sobre los sistemas de eliminación dominantes". *Cfr.* N. ELKIN-KOREN, "Contesting algorithms: restoring the public interest in content-removal AI", *Big Data & Society*, July 2020 (https://journals.sagepub.com/doi/full/10.1177/2053951720932296).

8. Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política. Por razón de extensión no se va a analizar este texto, aunque hay referencias expresas a este instrumento en marco jurídico sí analizado. Sobre el particular puede verse, P. VILLASCHI, "The Regulation of Political Targeting in the Italian and European Union Legal Framework", *Rivista di diritto internazionale privato e Processuale (RDIPP),* Gennaio-Marzo 2024, pp. 136 ss.; donde se analiza la regulación del *targeting* político desde el punto de vista del sistema y de la Unión Europea. Desde el Derecho de la Unión se realiza este estudio a la luz de la DSA y de la propuesta del Reglamento. En particular, este trabajo trata de analizar si estas reglas (las vigentes y el texto propuesto) podrían ser una respuesta a la focalización política, frenando el poder de los nuevos guardianes del ciberespacio y garantizando los derechos de los usuarios.

9. Como es el caso del Consejo de Europa, en cuyo ámbito se ha aprobado ya el Primer Tratado Global sobre Inteligencia Artificial, que acompaña a los ya existentes trabajos sectoriales del Consejo. *Vid.* Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (acuerdo conocido como *Framework Convention, CETS n.º 225*), de 17 de mayo de 2024, firmado por la UE,

en cuanto al ajuste a esta realidad que es la IA (no solo la vigente sino en atención a su potencial desarrollo) y manifestar deficiencias significativas como instrumentos suficientes para conseguir la tan deseada seguridad jurídica para todos los agentes implicados[10]. A la delimitación del potencial marco jurídico europeo aplicable al objeto de estudio se dedicará el siguiente apartado. Para finalizar el trabajo, como tercer bloque, se aproximará la cuestión desde la perspectiva de los mecanismos concretos de lucha contra la desinformación en el uso de los servicios digitales (esencialmente de intermediación) dentro de la UE. Se prestará especial atención a las obligaciones de los prestadores de servicios en línea impuestas por la DSA, en corregulación con otras fuentes (entre las que destacan aquellas de carácter autorregulatorio).

II. MARCO JURÍDICO EUROPEO FRENTE A LOS RIESGOS DEL USO DE LA IA

4. La UE, dentro de sus acciones para la soberanía digital, ha aprobado varias iniciativas en el marco regulatorio de la IA optando por distintas técnicas legislativas. Dentro de estas iniciativas institucionales destaca el Reglamento sobre inteligencia artificial (Reglamento de IA o Ley de IA)[11]. En este instrumento se articulan los principales requisitos y obligaciones para los proveedores, desarrolladores e implementadores de IA, cuando afecten al mercado interior, en relación con los usos específicos de la IA[12],

---

EEUU, Reino Unido, Andorra, Georgia, Islandia, Noruega, la República de Moldavia, San Marino e Israel. https://www.coe.int/en/web/conventions/full-list?module=-treaty-detail&treatynum=225

10. Sin olvidar el objetivo de promover la innovación dentro de la UE.

11. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican los Reglamentos (CE) 300/2008, (UE) 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial). Un análisis del nuevo Reglamento de Inteligencia Artificial, aprobado el 13 de marzo del 2024 en la reglamentación de los distintos usos de la Inteligencia Artificial para limitar los riesgos que de estos se pueden derivar, en A. RUIZ FORNS, A. NICOLÁS "Nuevo Reglamento Europeo de Inteligencia Artificial", *Diario La Ley*, ISSN 1989-6913, N.º 10491, 2024. Sobre las diferentes propuestas previas al texto definitivo durante el año 2021, en particular sobre los fundamentos y contenido de la Propuesta de abril de 2021, su ámbito de aplicación, su interacción con otras disposiciones del Derecho de la Unión, los mecanismos previstos para su aplicación, así como las principales cuestiones en la materia que quedan al margen de la Propuesta. P. A. DE MIGUEL ASENSIO, "Propuesta de Reglamento sobre inteligencia artificial", *La Ley Unión Europea*, número 92, 2021.

12. En las distintas versiones de la propuesta de Reglamento IA, hasta el texto definitivo, la obligación de que ciertos sistemas y modelos de IA dispongan de una "documentación

abordado desde un enfoque basado en los riesgos[13]. Junto con el Reglamento se articulan Directivas sobre responsabilidad en materia de IA, de necesaria transposición por los Estados miembros; estos instrumentos también deben referirse en el contexto del estudio propuesto, en la medida que haya que establecer la responsabilidad derivada del funcionamiento de los sistemas de IA en esta materia (como producto defectuoso o a través de la responsabilidad extracontractual derivada de su uso).

5. En primer lugar, se analizarán los principales instrumentos que conforman el marco regulatorio específico de la IA en la UE, por cuanto que esta tecnología sea la utilizada para llevar a cabo la eventual actividad de desinformación que se difunde a través de las plataformas digitales. El conjunto de normas que deben referirse se completa con la DSA, toda vez que el tratamiento o generación de contenidos por la IA, que pueden participar en la labor de desinformación, se realiza o difunde a través de plataformas digitales/buscadores sujetos a este instrumento si dirigen sus servicios en línea dentro de la UE. Este instrumento, junto con los propios de la IA, determinan las obligaciones que en este ámbito pueden imponerse a estos operadores y las consecuencias en su régimen de responsabilidad en este tipo de casos.

1. EL REGLAMENTO DE IA: SISTEMAS DE IA PARA LA DESINFORMACIÓN ¿SISTEMAS PROHIBIDOS, ALTO RIESGO O RIESGO MODERADO?

6. El Reglamento de IA es la primera regulación integral de la IA en el mundo[14], aplicable a los desarrolladores e implementadores de IA que operen directa o indirectamente dentro de la UE (incluso si no prestan servicios

técnica" que explique cómo funcionan a nivel interno se mantiene. Desde el punto de vista jurídico, han de abordarse sus implicaciones en caso de litigio de responsabilidad civil, siendo una cuestión más que significativa. Un análisis de esta obligación desde un punto de vista técnico y jurídico puede verse en P. DE ARTIÑANO MARRA, J. SÁNCHEZ ORO, "Responsabilidad por el funcionamiento de sistemas de inteligencia artificial: los desafíos de la 'documentación técnica' del Reglamento de Inteligencia Artificial", *Derecho Digital e Innovación. Digital Law and Innovation Review*, N.º 20, 2024.

13. Sigue así la aproximación proteccionista respecto a la información de los ciudadanos europeos, ya recogida en instrumentos anteriores como es el Reglamento General de Protección de Datos. Reglamento (UE) 2016/679 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. *Cf.* M. BARRIO ANDRÉS, "El efecto Bruselas del Reglamento Europeo de inteligencia artificial", *OTROSÍ.: Revista del Colegio de Abogados de Madrid*, N.º 2, 2024, pp. 47-48.

14. Una visión comparada de los sistemas regulatorios de la IA desde la perspectiva de la UE, OCDE y EEUU, en PADÍ, A. "Así se está regulando la IA en la UE, EE.UU. y la OCDE: el difícil equilibrio entre seguridad y fomento de la innovación", 23.02.2024 (https://

cubiertos en el mercado interior sino en terceros Estados, siempre que se trate de sistemas de alto riesgo, cuando los resultados de salida generados por dichos sistemas estén destinados a utilizarse en la Unión[15], o con establecimiento en terceros Estados cuando introduzcan en el mercado, presenten servicio o se utilicen en la UE)[16], en todas sus disposiciones a partir de 2 de agosto de 2026[17]. Este Reglamento forma parte de un paquete europeo más amplio de medidas políticas para fomentar el desarrollo de una IA fiable, que también incluye el paquete de innovación en materia de IA[18] y el plan coordinado sobre IA[19]. En conjunto, estas medidas tratan de garantizan la seguridad y los derechos fundamentales de las personas y las empresas en lo

www.garrigues.com/es_ES/garrigues-digital/asi-esta-regulando-ia-ue-eeuu-ocde-dificil-equilibrio-seguridad-fomento)

15. Los sistemas de IA de alto riesgo deben entrar en el ámbito de aplicación del Reglamento aunque no se introduzcan en el mercado, se pongan en servicio, ni se utilicen en la Unión. *Vid.* considerando 22, donde se recoge el ejemplo paradigmático de supuesto que cae dentro de su ámbito de aplicación en estas circunstancias: cuando un operador establecido en la Unión firma con un operador establecido en un tercer país un contrato para la prestación de determinados servicios en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo. En dichas circunstancias, el sistema de IA usado en un tercer país por el operador podría tratar datos recabados lícitamente en la Unión y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión los resultados de salida generados por dicho sistema de IA a raíz de este tratamiento sin que el sistema de IA de que se trate se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar soslayar la aplicación de este instrumento en estos casos, el Reglamento también debe aplicarse a los proveedores y responsables del despliegue de sistemas de IA establecidos en un tercer país, en la medida en que los resultados de salida generados por dichos sistemas estén destinados a utilizarse en la Unión.
16. *Vid.* Art. 2. Sobre el ámbito de aplicación espacial del Reglamento y su impacto en las actividades de las organizaciones con sede fuera de la UE; en concreto, en relación con los sujetos involucrados y el efecto extraterritorial, véase M. BARRIO ANDRÉS, "Consideraciones sobre el ámbito extraterritorial del Reglamento Europeo de Inteligencia Artificial", *Derecho Digital e Innovación. Digital Law and Innovation Review*, N.º 20, 2024; A. ORTEGA GIMÉNEZ, "La extraterritorialidad del futuro Reglamento Europeo de Inteligencia Artificial", *Revista jurídica Colex*, N.º 36, 2024, pp. 22-23.
17. *Vid*. art. 113. El Reglamento de IA entró en vigor el 1 de agosto de 2024 y será plenamente aplicable 2 años después, con algunas excepciones: las prohibiciones se aplican a los seis meses, las normas de gobernanza y las obligaciones para los modelos de IA de uso general serán aplicables a los doce meses y las normas para los sistemas de IA —integrados en productos regulados— se aplicarán al cabo de treinta y seis meses.
18. Aprobado por la Comisión con el fin de apoyar a Pymes y Startups sobre IA, en marcha desde enero de 2024 (iniciativa GenAI4EU). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383
19. El Plan Coordinado sobre Inteligencia Artificial tiene por objeto acelerar la inversión en IA, aplicar estrategias y programas de IA y armonizar la política de IA para evitar la fragmentación en Europa (https://digital-strategy.ec.europa.eu/es/policies/plan-ai)

que respecta a la IA y al mismo tiempo reforzar la adopción, la inversión y la innovación en IA en toda la UE —e incluso fuera de ella—; cuestión distinta es el alcance de sus disposiciones y la eficacia regulatoria de esta realidad[20]. Consecuentemente, el objetivo de esta norma es doble. Por un lado, garantizar que los sistemas de IA introducidos en el mercado europeo y utilizados dentro de la Unión sean seguros y respeten los derechos fundamentales y los valores de la UE. Por otro, promover la inversión e innovación en IA y facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones que utilicen este tipo de sistemas.

7. Expuestas las potenciales bondades del instrumento, procede determinar si resulta o no aplicable al tipo de sistemas de IA que permiten el tratamiento o generación de contenidos que pueden utilizarse con el objetivo de desinformar que son publicados y difundidos en redes sociales. El Reglamento opta (como es usual en este tipo de instrumentos) por utilizar conceptos autónomos e independientes para delimitar su ámbito de aplicación; por lo que es necesario referir la definición de sistema de IA recogido a tales efectos. El art. 3 numeral 1.º define "sistema de IA" como "un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales". Esta amplia definición permite encajar sin problemas aparentes, tanto las aplicaciones de IA generativa, como son las conocidas en términos generales como *deepfakes* (de uso extendido para la generación de información falsa o manipulada con el objetivo de desinformar), como incluso los *bots* de redes sociales; pero también los sistemas algorítmicos que permiten tomas de decisiones automatizadas. En consecuencia, el presupuesto del que se parte

20. Cabe observar otras aproximaciones de otros países en el intento de reglamentar o controlar esta realidad. Así, en EEUU se publicó la Orden Ejecutiva del presidente Joe Biden (norma con fuerza de ley) de fecha 30 de octubre de 2023. La *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, permite a las autoridades y propio gobierno estadounidense un nivel de injerencia muy alto en cuanto a la información que se trate y/o genere con la utilización de la IA. Otra diferencia importante con el sistema Europeo es que en el Reglamento europeo únicamente se define lo que es un "sistema de IA", EE.UU. opta por definir la propia "IA", el "modelo de IA" y el "sistema de IA". Un análisis de las líneas generales de la Orden puede verse en "El presidente Biden emite una orden ejecutiva para desarrollar en los EEUU una inteligencia artificial segura y confiable", *Diario La Ley*, 30/10/2023 (https://diariolaley.laleynext.es/dll/2023/10/31/el-presidente-biden-emite-una-orden-ejecutiva-para-desarrollar-en-los-eeuu-una-inteligencia-artificial-segura-y-confiable).

es que los sistemas de IA utilizados para generar información falsa o manipulada —potencialmente con el objetivo de desinformar—, como aquellos utilizados para tratar datos que puedan tener ese resultado, están cubiertos por el Reglamento de IA y habrá que clasificar de qué tipo de IA se trata(en función de los riesgos que generan) para concretar las condiciones y obligaciones que deben cumplirse dentro de la UE.

8. Aunque la mayoría de los sistemas de IA presentan un riesgo limitado o incluso inexistente, y pueden contribuir a resolver muchos retos sociales, también es cierto que determinados sistemas crean riesgos que deben regularse para evitar resultados indeseables —como aquellos vinculados a la toma de decisiones automatizadas a través de IA sin saber los criterios utilizados para ello, pero también el recurso a la IA para tratar o generar contenidos que contribuyan a la desinformación—. El Reglamento pretende abordar de manera suficiente los retos específicos que pueden plantear los sistemas de IA. Este instrumento es de aplicación obligatoria para todas las empresas de la Unión —o dirijan su actividad a ella— que sean proveedoras o usuarias de sistemas IA, e impone obligaciones y requisitos cuando la aplicación genere riesgo (especialmente si éste es alto). Las disposiciones de este nuevo instrumento se dirigen a varias cuestiones: 1) abordar los riesgos creados específicamente por las aplicaciones de IA; 2) prohibir las prácticas de IA que planteen riesgos inaceptables; 3) determinar una lista de aplicaciones de alto riesgo; 4) establecer requisitos claros para los sistemas de IA para aplicaciones de alto riesgo; 5) definir obligaciones específicas para los implementadores y proveedores de aplicaciones de IA de alto riesgo; 6) exigir una evaluación de la conformidad antes de que un sistema de IA determinado se ponga en servicio o se introduzca en el mercado; 7) aplicar el cumplimiento después de que se introduzca en el mercado un sistema de IA determinado; 8) establecer una estructura de gobernanza a escala europea[21] y nacional[22]. El cumplimiento de las reglas e imposiciones previstas

21. En la que se ubica la Oficina Europea de Inteligencia Artificial, creada en febrero de 2024 en el seno de la Comisión como parte de la estructura administrativa de la Dirección General de Redes de Comunicación, Contenido y Tecnologías. La Oficina supervisa el cumplimiento y la aplicación del Reglamento con los Estados miembros y tiene un papel de apoyo a las autoridades nacionales y europeas competentes en la aplicación de las normas sobre sistemas de IA. La creación de la Oficina no afectará a las competencias de las autoridades nacionales competentes (en caso de España, la Agencia Española de Supervisión de Inteligencia Artificial, AESIA) o de otros órganos de la UE en la supervisión de los sistemas de IA (https://digital-strategy.ec.europa.eu/en/policies/ai-office).

22. Desde la perspectiva española, el 22 de agosto de 2023 se aprobó el estatuto por el que crea la AESIA, con sede en A Coruña. La constitución efectiva tuvo lugar 3 meses

en el Reglamento no es sencillo, y parece que requiere de colaboración a tales efectos[23]. El propio instrumento indica que es deseable que existan herramientas, documentación y experiencia normativa desde la perspectiva nacional de los Estados miembros para su consecución (en este contexto se sitúan los Sandbox regulatorios de IA[24], como medidas previstas en el Cap. VI); así como el recurso —*mutatis mutandis*— a procedimientos previstos en otros instrumentos ya vigentes[25].

9. El marco regulador establecido por el Reglamento de IA parte de un enfoque basado en el riesgo, para lo que define cuatro niveles para los sistemas de IA: riesgo mínimo; riesgos limitados, alto riesgos y riesgo inaceptable. La clasificación y categorización de los sistemas de IA en cada uno de ellos condiciona el catálogo de obligaciones específicas que les son exigibles. Están directamente prohibidos todos los sistemas de IA considerados una clara amenaza para la seguridad, los medios de subsistencia y los derechos de las personas (como son aquellos que establece la puntuación social por

---

después de la entrada en vigor, a finales de noviembre de 2023. España es el primer país europeo en tener un organismo regulador de IA, que sumirá en nuestro país todas aquellas materias y competencias que deben ser tomadas en materia de IA como Estado Miembro.

23. Para facilitar la transición al nuevo marco regulador (hasta la plena aplicación), la Comisión ha puesto en marcha el Pacto sobre la IA: una iniciativa voluntaria con el fin de apoyar la futura aplicación e invita a los desarrolladores de IA de Europa y de fuera a cumplir con antelación las obligaciones clave del Reglamento. El Pacto de la IA se estructura en torno a dos pilares. Pilar I: Recopilación e intercambio con la red del Pacto de IA. Pilar II: facilitar y comunicar los compromisos de las empresas. https://digital-strategy.ec.europa.eu/en/policies/ai-pact

24. En España, el RD 817/2023, de 8 de noviembre, habilita al Ministerio de Asuntos Económicos y Transformación Digital, a través de su Secretaría de Estado de Digitalización e Inteligencia Artificial, a abrir la convocatoria a empresas para participar en el entorno controlado de pruebas (*Sandbox*) del Reglamento IA. Es un proyecto piloto, encabezado por España y respaldado por la Comisión Europea, que tiene como objetivo producir directrices de buenas prácticas y guías para concienciar a las empresas, con un enfoque particular en las pymes y startups, de cara a facilitar la adopción por su parte de sistemas de inteligencia artificial en cumplimiento con el Reglamento IA.

25. Así se hace remisión expresa al Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) 305/2011). En particular, en relación con la supervisión y vigilancia de los sistemas de IA que se basen en modelos de IA de uso general. Así, a modo de ejemplo, se remite expresamente al procedimiento de asistencia mutua transfronteriza previsto en el capítulo VI del Reglamento 2019/1020, para aclarar las responsabilidades y competencias a escala de la Unión y nacional en lo que respecta a los sistemas de IA que se basan en modelos de IA de uso general (Considerando 161 Reglamento IA).

parte de los gobiernos[26], hasta los juguetes que utilizan asistencia de voz que fomentan comportamientos peligrosos, por ejemplo aquellos que animen al suicidio)[27]. En este sentido, en relación con tema objeto de estudio, si se toma como referencia el tenor del Considerando 29 del Reglamento IA cabría concluir —en términos generales y para determinados casos aunque no esté expresamente recogido— que el uso de sistemas de IA con el fin de desinformar conduciría a que ese tipo de sistemas pudiera resultar prohibido dentro de la UE. Así, se indica que "*las técnicas de manipulación que posibilita la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente. Son especialmente peligrosos y, por tanto, deben prohibirse la introducción en el mercado, la puesta en servicio o la utilización de determinados sistemas de IA con el objetivo o al efecto de alterar de manera sustancial el comportamiento humano, con la consiguiente probabilidad de que se produzcan perjuicios considerables, en particular perjuicios con efectos adversos suficientemente importantes en la salud física o mental o en los intereses financieros*". Esa referencia en particular a los supuestos más graves no es excluyente de otros posibles resultados no deseables respecto de intereses, no sólo particulares, sino teniendo en cuenta intereses generales, como son la democracia o seguridad nacional; por ejemplo, cuando esa desinformación se dirige a desestabilizar un sistema democrático en contexto de procesos electorales (particularmente en el ámbito de votaciones telemáticas). Esta eventual posibilidad sólo podría fundamentarse de manera razonada cuando se trate de sistemas o modelos fundacionales creados con el fin concreto o al efecto de alterar de manera sustancial el comportamiento humano, como técnica de manipulación para fines ilícitos —lo que no parece pueda afirmarse en términos generales para todos aquellos sistemas que por sus características potencialmente pudieran utilizarse para estos fines, aunque no hubieran sido diseñados para ello—.

26. El llamado "*social scoring*", que mediante IA permite puntuar a los ciudadanos, calificando las autoridades a estos en función de su comportamiento social. La evaluación del comportamiento de las personas se realiza mediante la recopilación masiva de datos personales. Países como China ya han implementado sistemas similares, que permiten a las autoridades calificar a sus ciudadanos en función de su comportamiento social y financiero, lo que podría llevar a discriminaciones o castigos injustificados. En la medida que el uso de este tipo de sistemas de IA puede tener resultados discriminatorios y abocar a la exclusión a determinados colectivos quedan todos ellos prohibidos a la luz del Reglamento. *Vid*. Cdo. 31.

27. Quedando prohibidas en particular todos los sistemas de IA que pueden utilizarse en el ámbito de la garantía del cumplimiento del Derecho. *Vid*. considerandos 28-33, Reglamento IA. Dejando al margen aquellos sistemas de IA que se pongan en servicio o se utilicen, con o sin modificación, con fines militares, de defensa o de seguridad nacional, que se excluyen del ámbito de aplicación del Reglamento (Cdo. 24, art. 3.2.II).

10. En términos generales, los sistemas de IA (generativa) que permitan el tratamiento o creación de contenidos utilizados con el fin de desinformar podrían potencialmente encajar tanto dentro de los sistemas o modelos de alto riesgo como de riesgo moderado, en atención a la descripción que el Reglamento ofrece para la calificación en este nivel de la tecnología de IA, en función de las circunstancias concurrentes. No obstante, como se verá, salvo supuestos muy concretos, los sistemas generativos o modelos fundacionales de IA que permiten crear contenidos que pueden no ser reales, típicamente encajarán dentro de riesgos moderados (sistemas de riesgos no elevados).

11. Los sistemas de IA identificados como de alto riesgo (Cap. III), son aquellos que generan un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas[28], influyendo sustancialmente en el resultado de la toma de decisiones[29]. Son aquellos sistemas que incluyen la tecnología de IA utilizada en: 1) Biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable (por ejemplo, destinados a ser utilizados para el reconocimiento de emociones); 2) infraestructuras críticas (por ejemplo, el transporte, suministro de agua, electricidad, etc.), que podrían poner en peligro la vida y la salud de los ciudadanos; 3) formación educativa o profesional, que puede determinar el acceso a la educación y el curso profesional de la vida de una persona (por ejemplo, puntuación de los exámenes); 4) componentes de seguridad de los productos (por ejemplo, aplicación de IA en cirugía asistida por robot); 5) empleo, gestión de trabajadores y acceso al trabajo por cuenta propia (por ejemplo, *software* de clasificación de currículos para procedi-

28. Los sistemas de IA clasificados como de alto riesgo deben cumplir una serie de requisitos concretos (Secc. 2, Cap. III) antes de que puedan introducirse en el mercado interior: contar con sistemas adecuados de evaluación y mitigación de riesgos; alta calidad de los conjuntos de datos que alimentan el sistema para minimizar los riesgos y los resultados discriminatorios; registro de la actividad para garantizar la trazabilidad de los resultados; documentación detallada que proporcione toda la información necesaria sobre el sistema y su finalidad para que las autoridades evalúen su conformidad; información clara y adecuada al implementador; medidas adecuadas de supervisión humana para minimizar el riesgo; alto nivel de robustez, seguridad y precisión. Además de las condiciones o requisitos previos, se establece en la Sección 3 del Cap. III (arts. 16 a 27) las obligaciones que este respecto deben cumplir los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes (en atención a las responsabilidades exigidas a lo largo de la cadena de valor de la IA), sobre el control, supervisión y evaluación de riesgos de este tipo de sistemas —a este respecto, serían relevantes las obligaciones vinculadas a la evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo recogidas en el art. 27—.

29. Art. 6 y Anexo III (en relación con art. 6.2).

mientos de contratación); 6) servicios públicos y privados esenciales (por ejemplo, calificación crediticia que niega a los ciudadanos la oportunidad de obtener un préstamo); 7) aplicación de la ley que pueda interferir con los derechos fundamentales de las personas (por ejemplo, evaluación de la fiabilidad de las pruebas); 8) gestión de la migración, el asilo y el control fronterizo (por ejemplo, examen automatizado de las solicitudes de visado); 9) administración de justicia y procesos democráticos (por ejemplo, soluciones de IA para buscar resoluciones judiciales).

En este último punto, cabría plantearse si cuando la desinformación afecta a procesos democráticos en elecciones (nacionales o en instituciones supraestatales) los riesgos de injerencia externa permitirían clasificar los sistemas de IA que puedan utilizarse a estos fines como de alto riesgo. En este sentido se manifiesta expresamente el Anexo III[30] complementado por el considerando 62 del Reglamento. Así, sin perjuicio de las normas previstas en el Reglamento sobre transparencia y segmentación en la publicidad política, y con el objetivo de afrontar los riesgos de injerencia externa indebida en el derecho de voto garantizado en el artículo 39 de la Carta de Derechos Fundamentales de la UE[31] y de efectos adversos sobre la democracia y el Estado de Derecho, deben clasificarse como sistemas de IA de alto riesgo "*los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o un referéndum, o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos, con excepción de los sistemas de IA a cuyos resultados de salida las personas físicas no están directamente expuestas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico*". Consecuentemente, no es el fin último para lo que el sistema de IA se ha utilizado —en nuestro caso para crear esa desinformación destinada para influir en los resultados de procesos electorales— lo que permitiría calificar el sistema como de alto riesgo con todas las consecuencias[32]; lo relevante es el diseño mismo del sistema para esta finalidad específica y particular (por ejemplo, sistemas que manipulen el voto telemático, que suplanten la identidad de personas reales, que simulen ser personas reales con derecho a voto y en este sentido puedan emitir votos que computen en ese proceso electoral, etc.). Una aproximación en otro sentido supondría que cualquier sistema de IA gene-

30. Anexo III punto 8 letra b).
31. En adelante, CDFUE.
32. Tanto en lo que respecta a las específica imposiciones y obligaciones que se establece en el Reglamento de IA para este tipo de sistemas, como en relación con la carga de la prueba y nexo de causalidad (presunción del art. 4.1) que la propuesta de Directiva sobre responsabilidad extracontractual por el uso de IA (*infra.* Ap. II. 2.2).

rativo —o modelo fundacional— que permitiera la generación o tratamiento de información no real o manipulada (incluidas imágenes y contenido audiovisual[33]) estaría por esa razón dentro de esta clasificación, dado que potencialmente pueden operar para influir en un procedimiento electoral (cuando no fuera ésta su finalidad prevista[34] y aun siendo un uso indebido razonablemente previsible[35] del sistema). El resultado de esta calificación se traduce en obligaciones concretas respecto de los sistemas de alto riesgo (para el que lo ha introducido o desarrollado): 1) relativas a la previsión de un sistema de gestión de riesgos del art. 9: la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible[36]; 2) de transparencia y comunicación de información a los responsables del despliegue vinculado a la finalidad prevista dentro de las instrucciones de uso (art. 13.3) y de supervisión humana con el objeto de prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible (art. 14.2).

12. En términos generales, los sistemas IA de tratamiento o generación de contenidos que puedan utilizarse para la desinformación serán clasificados como sistemas de riesgo moderado o limitado —al margen de los supuestos analizados anteriormente—. El riesgo limitado se refiere a los riesgos asociados con la falta de transparencia en el uso de la IA (Cap. IV). El Reglamento de IA introduce obligaciones específicas de transparencia para garantizar que los seres humanos estén informados cuando sea necesario que la información o contenido publicado está generado por IA y no es actividad humana, fomentando la confianza (art. 50). Por ejemplo, cuando se

33. Entre otras herramientas de IA generativa de imágenes (a partir de texto), pueden referirse, a modo de ejemplo, *Stable Diffusion*, *Leonardo.ai*, *clipdrop.co*; o *Dall-E* de *Copilot* (Microsoft); otras herramientas como *Synthesia* pueden generar vídeos con personas sintéticas (avatares); la herramienta *Tortoise* permite generar audios.

34. entendida como el "uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica". *Vid*. art. 3 numeral 12, Reglamento IA.

35. Definido como "*la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas, incluidos otros sistemas de IA, razonablemente previsible*". Art. 3, numeral 13.

36. Lo que se puede vincular en estos casos con los riesgos sistémicos, su evaluación y adopción de medidas para su mitigación que se impone por la DSA a los grandes prestadores de servicios digitales y motores de búsqueda en relación con el uso inadecuado de sus servicios realizado por los usuarios.

utilizan sistemas de IA como los *chatbots*, las personas deben ser conscientes de que están interactuando con una máquina para que puedan tomar una decisión informada de continuar o dar un paso atrás. Además, los proveedores deben en todo caso garantizar que el contenido generado por la IA sea identificable. Asimismo, el texto generado por la IA publicado con el fin de informar al público sobre asuntos de interés público debe etiquetarse como generado artificialmente —lo que es esencial precisamente en el ámbito de la desinformación—. Esto también se aplica al contenido de audio y video que pueden constituir falsificaciones de la realidad y, por tanto, contribuir a la desinformación[37].

13. Cabe en este contexto de evaluación de riesgos (y su nivel) en el uso de sistemas de IA (o modelos de IA de uso general que pueden formar parte de esos sistemas de IA) plantearse si la desinformación es un riesgo sistémico a la luz del Reglamento, y las consecuencias de esta adjetivación. En el Reglamento IA se utiliza un concepto autónomo y propio de riesgos sistémicos —a diferencia de la DSA en la que no se contiene delimitación del término pero sí se recoge referencia expresa del mismo a través de ejemplos concretos en su articulado[38]—. Se define como riesgo sistémico un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor (art. 3 numeral 65). Se vincula este tipo de riesgos a modelos de IA de uso general (que pueden formar parte de los sistemas de IA, diferenciando así ambas figuras[39]), por lo que la delimitación de este tipo de modelos de IA (de uso general) es esencial. El modelo de IA[40] de uso general se define en el art. 3, numeral 63 como un modelo de IA "entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas

37. Sobre la posible exigencia de las obligaciones de etiquetado impuestas por el Reglamento de IA a las muy grandes plataformas digitales cuyos servicios se utilicen para generar y difundir contenido generado por IA, ante el riesgo de desinformación y en particular en el contexto de procesos electorales *vid. infra* apdo. III. 2.2.

38. *Vid*. art. 34 DSA. *Infra* Ap. III.1.1.

39. Siendo los sistemas de IA un concepto más amplio, omnicomprensivo, que puede abarcar distintos modelos de IA.

40. En términos generales, entendido como programa informático entrenado en algoritmos específicos que le ayudan a replicar la inteligencia humana para hacer predicciones, encontrar patrones y tomar decisiones.

distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado". Esta definición se vincula con la consiguiente de sistema de IA de uso general, como aquel sistema de IA basado en un modelo de IA de uso general que puede operar tanto como uso directo como de manera integrada en otros sistemas de IA[41].

La vinculación expresa de los riesgos sistémicos en el uso de la IA (modelos o sistemas de IA de uso general) con efectos negativos sobre los derechos fundamentales o a la sociedad en su conjunto, permitiría incluir como de esta categoría los eventuales supuestos de desinformación por contenidos generados por IA[42] que afectaran a procesos electorales (por ejemplo con el objeto influir en los resultados) o atenten contra la imagen o buen nombre de una persona (contenidos que atenten contra derechos fundamentales de la personalidad a la luz del art. 8 del CEDH, arts. 7-8 CDFUE). Esta aproximación se refuerza si se toma en consideración el tenor del Considerando 110 y los ejemplos que en este se recogen para ilustrar los riesgos sistémicos de los modelos de IA de uso general, entendido como cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios. El punto de partida o presupuesto es que los riesgos sistémicos aumentan con las capacidades y el alcance de los modelos, que pueden surgir durante todo el ciclo de vida del modelo y que se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la equidad y la seguridad del modelo, el nivel de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, las estrategias de divulgación y distribución, la posibilidad de eliminar las salvaguardias y otros factores. Particular interés ha de prestarse a los riesgos derivados de posibles usos indebidos intencionados o de problemas en materia de control —relacionados con la armonización— con la intención humana de resultados no deseados; especialmente a las maneras en que los modelos pueden dar lugar a sesgos dañinos y discriminación que entrañan riesgos para las personas, las comunidades o las sociedades, a la facilitación de la desinformación o el menoscabo de la intimidad. Todo ello supone una amenaza para los valores democráticos y los derechos humanos, con el potencial

41. *Vid*. Art. 3, numeral 66.
42. Para ello, sería necesario la clasificación de esos modelos (o sistemas) de IA de uso general como modelos de IA de uso general con riesgo sistémico (de conformidad con el art. 51 y según el procedimiento del art. 52).

riesgo de que un concreto acontecimiento o resultado en este ámbito dé lugar a una reacción en cadena con efectos negativos considerables que podrían afectar incluso a una ciudad entera, un ámbito de actividad entero o una comunidad entera.

14. Es esencial delimitar el ámbito subjetivo de aplicación del Reglamento IA. Todas las obligaciones o requisitos previos a la introducción al mercado de los sistemas de IA (en particular de alto riesgo), como posteriormente[43] las obligaciones de supervisión y seguimiento para la implementación y comercialización de los sistemas, así como de información sobre su funcionamiento[44] recogidas, vinculan a los operadores concretos que participan como proveedores, desarrolladores e implementadores de IA[45] en los términos previstos en la norma. No es extensible la aplicación de estas disposiciones a los usuarios finales de estos sistemas de IA. Consecuentemente, a los usuarios de *apps* o herramientas de IA que permitan tratar información o generar contenidos no reales —o manipular hechos— que contribuyan a la desinformación, no les es exigible el cumplimiento de las obligaciones de este marco normativo de la IA (ya que no tienen ninguna responsabilidad en la cadena de valor de la IA en los términos del instrumento[46]). Por ello, en principio, no cabría plantearse cuestiones de responsabilidad o exigencia a través del Reglamento IA para las plataformas digitales que utilizan los sistemas de IA para tratamiento de contenidos (moderación en sentido amplio o labores de curación a través de sistemas algorítmicos) o

43. Las obligaciones que el Reglamento impone requieren de una gestión continua de la calidad y del riesgo por parte de los proveedores de IA tras su incorporación al mercado. En particular, para modelos de IA de uso general, estableciendo obligaciones adicionales que incluyen la autoevaluación y la mitigación de los riesgos sistémicos, la notificación de incidentes graves, la realización de pruebas y evaluaciones de modelos, así como los requisitos de ciberseguridad.

44. Los proveedores e implementadores deben informar de los incidentes graves y de los fallos de funcionamiento de los sistemas de IA, de conformidad con el art. 55 (para los proveedores de modelos de IA de uso general con riesgo sistémico); y el art. 73 (obligación de notificación de los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión).

45. Aun siendo implementadores de IA, que en principio estarían dentro de su ámbito de aplicación, el Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional (art. 2.10).

46. Usuarios entre los que estarían las plataformas digitales, típicamente respecto de los sistemas de IA utilizados para ejercicio de sus funciones de moderación/curación (mecanismos automatizados algorítmicos). No obstante, respecto de los servicios que prestan a los usuarios digitales, pueden tener la consideración de proveedores de modelos de IA de uso general (donde se incluye la IA generativa), si se encuentra entre sus servicios digitales la creación de contenidos a través de esta tecnología.

por sus usuarios digitales que utilicen sistemas externos IA de generación de contenidos (no reales o manipulados) que se difundan a través de sus servicios digitales. En estos casos, las obligaciones que pudieran exigirse, en particular a las muy grandes plataformas y buscadores, estarían conectadas a los deberes de diligencia debida impuestos por la DSA en el marco de la mitigación de los riesgos sistémicos vinculados a la prestación de servicios. En conclusión, atendiendo al ámbito de aplicación subjetivo del Reglamento de la IA, típicamente las plataformas digitales que operan dentro de la UE, que puedan verse vinculadas por sistemas o modelos de IA, no estarían *per sé* dentro de los sujetos vinculados por el Reglamento de IA[47], por lo que su eventual responsabilidad debería articularse mediante el recurso a la DSA[48] (en relación con el cumplimiento de las obligaciones en ella impuestas para estos operadores en este ámbito) e incluso eventualmente a través de las eventuales Directivas sobre responsabilidad aplicables al uso de la IA.

2. DIRECTIVAS SOBRE RESPONSABILIDAD EN MATERIA DE IA

15. Con el propósito de reglamentar la eventual responsabilidad civil derivada del uso de la IA la Comisión Europea presentó dos propuestas legislativas a finales de 2022[49], que resultan de interés en el ámbito de estudio propuesto. La normativa hasta el momento existente en este sector (responsabilidad por productos) no estaba diseñada para abordar las particularidades de la IA, especialmente en lo que respecta al aspecto del aprendizaje automático (autoaprendizaje). Los sistemas de IA, al poder modificar su

47. Son operadores vinculados por las disposiciones de este Reglamento: el proveedor, el fabricante del producto, el responsable del despliegue, el representante autorizado, el importador o el distribuidor del sistema de IA cubierto (art. 3, en los términos indicados en los numerales 1.º a 8.º). Dejando al margen los supuestos de aquellas plataformas en línea y motores de búsqueda de muy gran tamaño cuyos servicios puedan utilizarse por sus usuarios para la creación de contenidos de IA generativa, en cuyo caso estarían vinculados por las obligaciones establecidas para los proveedores de modelos de IA de uso general, incluida la IA generativa. *Vid. Infra.* Apdo. III.2.2.

48. Quedan fuera de la DSA y cubierto por el Reglamento IA, las medidas de control de contenidos vinculado a la IA previsto por el propio sistema o modelo de IA —como por ejemplo, así ocurre en relación con el ChatGPT, en el que propios creadores tuvieron en cuenta la posible utilización del sistema para generar contenido lesivo que cause a personas o grupos de personas, como por ejemplo para hacer apología del terrorismo—, por lo que establecieron un moderador interno para bloquear el contenido potencialmente ofensivo. *Vid. infra*, Apdo. II. 3.

49. Estas dos propuestas forman parte del compromiso de la Comisión de promover la adopción de la IA de forma segura y fiable, en relación con el Libro Blanco sobre la IA publicado en 2020. Libro Blanco sobre la inteligencia artificial — un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19.2.2020. COM(2020) 65 final.

comportamiento sin intervención humana directa, generan lagunas jurídicas en lo que concierne a la atribución de responsabilidades cuando se generan daños. Precisamente la necesidad de reglamentar esas eventuales lagunas es lo que se pretendía por el legislador europeo con estas dos iniciativas[50], que se analizarán de manera separada en los siguientes apartados. En primer lugar, el texto de la ya aprobada nueva Directiva sobre productos defectuosos en relación con los posibles supuestos vinculados al objeto de estudio. Por otro lado, la propuesta de Directiva para la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA). Respecto de esta última, aunque finalmente ha sido retirada en febrero de 2025 por la Comisión, será analizada como base para una eventual propuesta futura revisada dada la necesidad de regulaciones que establezcan un marco claro de responsabilidad civil en sistemas de IA.

2.1. La Directiva de 2024 sobre productos defectuosos y su posible aplicación al caso

16. La primera de las propuestas se concreta en el ámbito de la responsabilidad por productos defectuosos, con el objeto de revisar el principal instrumento en la materia: la Directiva 85/374/CEE[51], para adaptarla a estos nuevos retos[52]. La Directiva (de 1985) no cubría las categorías de productos derivados de los sistemas de IA, por razones obvias[53]. En consecuencia, las normas recogidas en este instrumento no proporcionaban herramientas suficientes, y de manera clara, para poder determinar la eventual responsabilidad en este contexto; como puede ser, por ejemplo, la responsabilidad

50. Que buscaban responder a estas nuevas realidades proporcionando un marco que garantice una mayor seguridad jurídica, transparencia y un equilibrio justo entre los intereses de las empresas desarrolladoras de IA y los derechos de los usuarios.

51. Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos. DO L 210 de 7.8.1985, p. 29-33.

52. En el año 2018 el Consejo Europeo emitió un documento de evaluación de la Directiva de 1985 (*Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products*, Bruselas, 7 de mayo de 2018). De ese documento parte la Propuesta de Directiva del Parlamento europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. COM/2022/495 final.

53. Como constató la Comisión: *Questions and answers on the revision of the Product Liability Directive, European Commission, Brussels, 28 September 2022.* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5791 (Consultado el 4 de noviembre de 2024).

por daños causados por defectos en actualizaciones de *software*, por los algoritmos de aprendizaje automático utilizados o en los servicios digitales esenciales para el funcionamiento de un producto[54]. El objetivo de esta propuesta se centra, de esta suerte, en tratar de garantizar unas nuevas normas sobre responsabilidad por productos defectuosos que se adapten a los nuevos tipos de productos derivados del uso de la IA (lo que se puede vincular a esa nueva realidad conocida como el Internet de las cosas). Esta propuesta fue finalmente aprobada el pasado 12 de marzo de 2024 derogando la Directiva 85/374/CEE, recogiendo importantes variaciones en los procedimientos por productos defectuosos en relación con su predecesora. La nueva Directiva de 2024[55] establece un nuevo marco jurídico europeo de responsabilidad, que trata de adaptarse a los a los avances tecnológicos[56], los nuevos modelos de negocio de la economía circular[57] y el carácter cada vez más mundial de las cadenas de suministro. Otro eje esencial de esta actualización aborda las dificultades a las que se enfrentan las personas perjudicadas a la hora de reunir pruebas para demostrar la responsabilidad, especialmente cuando se trata de nuevas tecnologías. Estas nuevas normas sobre responsabilidad por productos defectuosos no solo benefician a los consumidores[58], sino que también buscan fomentar la implantación y

54. Del mismo modo, la regulación no permitía determinar quién es el responsable cuando una empresa modifica sustancialmente un producto que ya está en el mercado, o cuando un producto ha sido importado directamente desde fuera de la UE por un consumidor, lo que dificultaba la evaluación por parte de las empresas de los riesgos de la comercialización de productos innovadores, y dejaba a las víctimas de los daños sin la posibilidad de compensación para un número cada vez mayor de productos.

55. El día 10 de octubre de 2024 el Consejo aprobó el texto definitivo de la Directiva (UE) 2024/2853 del Parlamento europeo y del Consejo, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. La Directiva entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*. Los Estados miembros disponen de dos años para incorporar las disposiciones de la Directiva a su ordenamiento jurídico interno. DOUE-L-2024-81701

56. A este respecto, para adaptarse a la economía digital, la nueva Directiva amplía la definición de "producto" a los archivos de fabricación digital y los programas informáticos. Al igual que cualquier otro operador económico, cuando actúen como tal, las plataformas en línea también pueden ser consideradas responsables en relación con un producto defectuoso vendido en su plataforma (art. 4.1 y Considerandos 13 a 18).

57. Cuando la reparación o mejora de un producto se lleve a cabo al margen del control del fabricante original, la empresa o persona que modificó el producto debe ser considerada responsable a la luz de esta nueva Directiva (art. 8.2).

58. Son tres cuestiones esenciales en este sentido. Por un lado, se facilita el derecho a indemnización al garantizar que las personas perjudicadas que reclamen una indemnización ante un órgano jurisdiccional nacional puedan solicitar acceso a las pruebas pertinentes de que disponga el fabricante para acreditar la reclamación. En segundo

aceptación de nuevas tecnologías y proporcionan a los fabricantes claridad jurídica y unas condiciones de competencia equitativas[59].

17. Por lo que respecta a la posible responsabilidad en este ámbito vinculada al uso de la IA, de conformidad con la nueva Directiva de 2024, ésta queda incluida dentro del nuevo y más extenso concepto de "producto": entendido como "cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble", así como "la electricidad, los archivos de fabricación digital y los programas informáticos"[60]. De esta manera, se garantiza que las personas gocen de la misma protección, independientemente de que el producto defectuoso que les perjudique sea tangible o digital. No obstante, la información no debe considerarse un producto, por lo que las normas sobre responsabilidad por productos defectuosos no deben aplicarse al contenido de los archivos digitales, como los archivos multimedia o los libros electrónicos o el mero código fuente de los programas informáticos (Considerando 13). Consecuentemente, los contenidos digitales (publicados o difundidos a través de las plataformas online) tratados o generados por IA que puedan ser lesivos o atentativos de derechos y/o libertades fundamentales —ya sean individuales o colectivos— quedarían fuera del concepto de producto a efectos de esta Directiva. De esta suerte, la eventual responsabilidad que pueda exigirse por el perjudicado deberá canalizarse a través de las reglas aplicables en materia contractual o extracontractual (delictual o cuasidelictual), en función de la relación existente entre la supuesta víctima y el que resulte pasivamente legitimado. Típicamente, el

---

lugar, precisamente para la consecución de la indemnización debida, la novedad se vincula a la carga de la prueba: cuando el consumidor perjudicado encuentre dificultades excesivas para demostrar el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, el órgano jurisdiccional puede decidir que el demandante solo tenga obligación de demostrar la probabilidad de que el producto fuera defectuoso o de que el defecto haya causado el daño. Por último, a fin de garantizar que los consumidores europeos sean indemnizados por los daños ocasionados por un producto fabricado fuera de la UE, podrán ser considerados responsables por los daños la empresa importadora del producto o el representante en la UE del fabricante extranjero.

59. Un análisis de las principales novedades y del procedimiento de producto defectuoso derivados de esta Directiva, puede verse E. BUITRÓN; K. CARRIÓN y M. GONZÁLEZ, "Aprobación por el Parlamento Europeo de la propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos", *El Derecho — Procesal*, Secc. Tribuna, 10.04.2024 (https://elderecho.com/aprobacion-por-el-parlamento-europeo-de-la-propuesta-de-directiva-sobre-responsabilidad-por-los-danos-causados-por-productos-defectuosos#67234cb9f3c9e).

60. Deja de ser "cualquier bien mueble, excepto las materias primas agrícolas y los productos de la caza", como aparece en la Directiva de 1985 (art. 2).

demandado será el autor material del contenido lesivo o aquél que deba o pueda responder por los actos de aquél (actos de terceros)[61], ya sea porque ostente la potestad de "control" o "edición" sobre el contenido, o porque la responsabilidad se derive del incumplimiento de ciertos deberes de diligencia debida exigibles —de evaluación y mitigación de riesgos, supervisión y moderación de contenidos…— impuestos por la normativa aplicable a determinados operadores. En este último caso es donde encajaría la eventual responsabilidad de las plataformas digitales a través de las que se difunda la información (generada por IA), incluso si son prestadores de servicios de la sociedad de la información de intermediación[62]; en atención al cumplimiento de las obligaciones sustantivas que la DSA impone a estos agentes, en particular a las muy grandes plataformas y motores de búsqueda[63]. Cuestión distinta es que como resultado de ese funcionamiento defectuoso (no seguro por incumplir los requisitos de ciberseguridad exigidos, como veremos a continuación) de los sistemas de IA como producto (en términos amplios, incluyendo aquellos interconectados, en especial, en el ámbito del internet de las cosas) la información que se publica y difunde a través de las plataformas digitales sean datos personales (información íntima y personal) recabados por estos sistemas. En estos casos, sí que se podría exigir responsabilidad de conformidad con esta Directiva a los responsables de esa IA (como producto) cuyo funcionamiento defectuoso (por no ser seguro) ha traído como resultado la publicación de esa información[64]. Otra cuestión es la determinación de quién/es son los responsables de estos daños a la luz de este instrumento, que en ningún caso correspondería a las plataformas digitales de intermediación a través de las que se difunden estos datos.

61. Dejando al margen eventuales acciones judiciales que buscan otras pretensiones que no sean indemnizatorias o pecuniarias (compensación, reparación, sustitución), como son aquellas que pretenden la retirada del contenido o el bloqueo a su acceso; en cuyo caso la legitimación pasiva no se limita a los eventuales responsables del daño (o quienes deban responder como aquellos) sino que pueden ejercitarse frente a los prestadores digitales de intermediación cuyos servicios han sido utilizados para difundir o publicar el contenido controvertido (de conformidad con la normativa europea).

62. Lo que supone, en principio, que gozan de la condición de puerto seguro dentro del mercado interior, con un régimen de exención condicionada de responsabilidad por los actos realizados por los usuarios de sus servicios en línea prestados dentro de la UE.

63. *Vid. infra* Ap. III.1. Dada la vinculación que puede establecerse entre el régimen de responsabilidad de los prestadores de servicios digitales y el cumplimiento del catálogo de obligaciones sustantivas que la DSA impone a este tipo de operadores que presten sus servicios dentro del mercado interior. A este respecto, en profundidad, véase, C.I. CORDERO ÁLVAREZ, "El régimen de responsabilidad de las plataformas online en la DSA…", *ob. cit.*

64. Al margen de la entrada en aplicación de manera concurrente de la normativa de protección de datos personales.

18. En lo que respecta a los eventuales responsables de esos productos defectuosos vinculados a la IA, los desarrolladores o productores de programas informáticos, incluidos los proveedores de sistemas de IA en el sentido del Reglamento de IA, deben ser tratados como un fabricante[65]; por lo que se consideran responsables (Operadores económicos responsables de los productos defectuosos) de conformidad con el art. 8. La nueva redacción elimina la referencia directa al "productor", estableciendo en su lugar un listado de "operadores económicos responsables de los productos defectuosos", entre los que se incluyen el fabricante, el importador, el representante autorizado, el prestador de servicios de tramitación de pedidos a distancia o el distribuidor; de forma que el consumidor siempre pueda dirigirse a un agente en territorio europeo a quien pueda imputarse la responsabilidad. En consecuencia, la potencial responsabilidad de los proveedores de sistemas de IA[66], como fabricante del producto a los efectos de la nueva Directiva, cubrirá también cualquier daño causado por un componente defectuoso cuando esté integrado en un producto bajo su control[67] o esté interconectado con él[68] (lo que es significativo, por ejemplo, en el referido ámbito del Internet de las cosas). Este régimen de responsabilidad del que puede beneficiarse los consumidores aplica frente a operadores económicos con sede en la UE, aunque el producto (vinculado con la IA) se fabricó fuera del territorio de la Unión. En este sentido, el Considerando 37 de la nueva Directiva establece

65. *Vid*. considerando 13, en relación con el art. 4 numeral 10 de la nueva Directiva 2024.
66. Que de conformidad con el reglamento de IA un proveedor de un sistema de IA es cualquier persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente (art. 3 numeral 3 Reglamento IA). No obstante, para sistemas de IA alto riesgo se considera proveedor a cualquier distribuidor, importador, responsable del despliegue u otro tercero que, por tanto, debe asumir todas las obligaciones pertinentes (Considerando 84, Reglamento IA).
67. *Vid*. Considerando 18: "*Los servicios conexos y otros componentes, incluidas las actualizaciones y mejoras de programas informáticos, deben considerarse bajo el control del fabricante cuando estén integrados en un producto o interconectados con él, o suministrados por el fabricante, o cuando el fabricante autorice o consienta su integración, interconexión o suministro por parte de un tercero, por ejemplo cuando el fabricante de un aparato doméstico inteligente consienta en que un tercero facilite actualizaciones de programas para el aparato del fabricante o cuando un fabricante presente un servicio conexo o componente como parte del producto aunque sea suministrado por un tercero. No debe considerarse que un fabricante haya dado su consentimiento a la integración o interconexión simplemente por prever la posibilidad técnica de la integración o interconexión, por recomendar determinadas marcas o por no prohibir posibles servicios conexos o componentes*".
68. *Vid*. art. 8, numeral 1.º letra b), Directiva 2024.

que *"a fin de garantizar que las personas perjudicadas tengan posibilidad de reclamar una indemnización legalmente exigible cuando un fabricante esté establecido fuera de la Unión, debe ser posible exigir responsabilidades al importador del producto y al representante autorizado del fabricante designado para funciones específicas en virtud de la legislación de la Unión, por ejemplo la relativa a la seguridad de los productos y vigilancia del mercado"*. Esto ha de vincularse con el Reglamento de IA, en el que se establece que para los sistemas de IA de alto riesgo se considerará proveedor a cualquier distribuidor, importador, responsable del despliegue u otro tercero (Considerando 84, Reglamento IA). De esta suerte, frente a cualesquiera de estos operadores con sede en la UE vinculados al sistema de IA conectado al producto, o componente del producto o interconectado al producto defectuoso (aun fabricado en tercer Estado) podrá exigirse responsabilidad de conformidad con la nueva Directiva.

19. También resulta muy relevante la noción o criterio utilizado por la Directiva para determinar cuándo un producto es defectuoso —del que puede derivarse esa responsabilidad por los daños personales o materiales causados—. Si bien la nueva Directiva no varía en este aspecto, al definir un producto como defectuoso si no ofrece la seguridad que legítimamente se espera de él[69], sí que incorpora factores relevantes para determinar esta condición a la lista no exhaustiva de elementos que deben tener en cuenta los tribunales a la hora de evaluar esta cuestión[70]. Entre otros factores, destaca la interconexión[71] o las funciones de autoaprendizaje de los productos o de adquisición de nuevas características tras su introducción en el mercado o su puesta en servicio[72] (Considerando 32). Por consiguiente, un fabricante que diseñe un producto con la capacidad de desarrollar un comportamiento inesperado (como son aquellos vinculados con la IA modelos de uso general) será responsable de todo comportamiento que cause daños, es decir, se extiende su responsabilidad tras su introducción en el mercado (interior) mientras esté bajo su control. El momento en que un producto deja de estar bajo el control del fabricante también debe tenerse en cuenta en la valora-

69. Considerando 30: "*Con objeto de proteger la salud y la propiedad de las personas físicas, el carácter defectuoso de un producto debe determinarse no por su falta de aptitud para el uso sino por no cumplir las condiciones de seguridad a que tiene derecho una persona o que se exige en virtud del Derecho de la Unión o nacional" (…).*

70. *Vid.* Considerandos 30 a 34 Directiva 2024.

71. Para lo que también debe tener en cuenta los efectos razonablemente previsibles de otros productos en el producto en cuestión, como por ejemplo en un sistema doméstico inteligente.

72. A fin de reflejar la expectativa legítima de que el programa informático de un producto y los algoritmos subyacentes estén diseñados de manera que se evite un comportamiento peligroso del producto.

ción de su seguridad. Asimismo, un producto también puede considerarse defectuoso debido a su vulnerabilidad en materia de ciberseguridad, por ejemplo cuando el producto no cumpla los requisitos de ciberseguridad debidos. En este sentido, si por ejemplo un sistema doméstico inteligente que interconecta varios aparatos entre sí (a través de IA) que recopile datos personales (hábitos, comportamientos, incluso imágenes personales de los miembros de la familia en su faceta privada) si su anormal funcionamiento permitiera que esa información sea utilizada de manera lesiva por terceros fuera del sistema (por ejemplo, permitiendo la publicación o difusión de esa información en plataformas digitales de manera que afecte a su intimidad, propia imagen o incluso al honor, utilizado para desinformar sobre una determinada persona con fines no legítimos), la persona afectada podría exigir responsabilidad al fabricante[73] por los daños causados por ese funcionamiento defectuoso del sistema.

Precisamente, otra novedad de la Directiva se vincula con la carga de la prueba y la presunción de defectuosidad del producto; lo que en estos casos puede resultar significativamente compleja para el perjudicado. Si bien se mantiene que la carga de la prueba recae sobre el perjudicado —que deberá probar el daño que se alega sufrido, el carácter defectuoso del producto y el nexo de causalidad entre ambos—, la nueva norma establece una "presunción de causalidad" (*presumption of causality*); de forma que podrá ser suficiente con que parezca razonablemente probable que existe un nexo causal entre el producto y el daño alegado (Cdo 33)[74]. La operatividad de presunciones en este sentido, en especial para potenciales daños personales, parece que podría coadyuvar de manera significativa para la consecución de las debidas indemnizaciones para los eventuales perjudicados por el funcionamiento anormal (defectuoso) de los productos vinculados a la IA.

20. No obstante, pese a los evidentes avances y beneficios para los usuarios perjudicados por productos vinculados con la IA que se desprenden de esta nueva normativa, su operatividad dentro del concreto objeto de estudio parece descartada (tanto para exigir eventual responsabilidad para las plataformas digitales como intermediarios como para los usuarios de estas redes que publican y difunden a través de esos servicios digitales los contenidos

73. En los términos expuestos: los desarrolladores o productores de programas informáticos, incluidos los proveedores de sistemas de IA en el sentido del Reglamento de IA.

74. El nuevo texto entiende que las presunciones de hecho constituyen un mecanismo común para aligerar las dificultades probatorias del demandante y permiten al órgano jurisdiccional basar la existencia de un defecto o de un nexo causal en la presencia de otro hecho probado, preservando al mismo tiempo los derechos del demandado.

lesivos o no deseados generados por IA que causan desinformación[75]). En particular, respecto de las plataformas digitales (y buscadores), partiendo de la delimitación de los destinatarios de las obligaciones impuestas y consecuente régimen de responsabilidad establecido en la nueva Directiva (operadores económicos responsables de los productos defectuosos del art. 8), parece que los espacios digitales donde la información falsa o manipulada intervenida por IA se difunde no encajan dentro de esta delimitación conceptual (art. 4 numeral 10, complementado por el Cdo. 13). A más, la exclusión de los contenidos digitales como producto a los efectos de la Directiva (al margen de las excepciones referidas vinculadas a datos personales y falta de seguridad debida del producto de IA cubiertos, en las que tampoco las plataformas resultarías responsables de los productos IA causantes) conduce a la misma conclusión. Tampoco fuera de su labor de meros intermediarios resultaría de aplicación este marco jurídico. Así, en lo que respecta a los resultados potencialmente lesivos que puedan generarse por el uso por parte de las plataformas digitales de sistemas de IA (sistemas algorítmicos para toma de decisiones automatizadas) su eventual responsabilidad no encajaría dentro de esta Directiva, al no ser igualmente los responsables de estos sistemas[76]. Por consiguiente, la eventual responsabilidad que en estos casos pudiera exigirse a las plataformas digitales (incluidos buscadores) no podría canalizarse a través de la nueva Directiva de 2024, pese a que el sistema de IA utilizado pueda encajar dentro de la nueva y ampliada definición de producto y se verificara su condición de defectuoso y pudiera establecerse (principalmente mediante presunción de causalidad) el nexo causal entre el producto y el daño alegado. Veremos a continuación a la luz de la siguiente iniciativa sí coadyuvaría a los efectos propuestos y, por tanto, si en un futuro constituiría parte del marco jurídico aplicable a la eventual responsabilidad de las plataformas digitales en caso de desinformación intermediada por IA (dejando al margen la eventual responsabilidad de los usuarios digitales de estos espacios por las actuaciones realizadas a través de sus servicios).

---

75. En la medida que no son operadores económicos responsables del producto utilizado (app o herramienta de IA) para generar el contenido, y que la información digital generada no se entiende como producto (defectuoso) a los efectos de la Directiva 2024.

76. Cabría cuestionarse la posible inclusión como responsables si pudiera probarse que por parte de estos operadores digitales se hubiera alterado conscientemente los sistemas algorítmicos del modelo para conseguir unos resultados concretos que pueda causar daños a interese particulares, colectivos o generales. Al margen de la eventual responsabilidad de los fabricantes (proveedores o desarrolladores del sistema o modelo de IA en la UE) por no evitar usos indebidos previsibles como estos (lo que los permite caracterizar como defectuosos), también las plataformas podrían en estos casos caer dentro del ámbito de aplicación de este instrumento, cuya imposición se establece a los operadores económicos de responsabilidad con independencia de la culpa (Cdos. 9 y 42).

2.2. Propuesta de Directiva de adaptación de las normas de responsabilidad extracontractual a la IA: oportunidad perdida[77]

21. El segundo de los textos normativos que ha de traerse a colación, en este potencial marco jurídico aplicable, es la ya retirada propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)[78], como complemento a la Directiva anterior —y sobre la base, con remisiones expresas contantes, al Reglamento IA—. El punto de partida de este instrumento era tratar de promover la introducción generalizada de una IA fiable que garantice que los perjudicados por daños causados por esta tecnología obtengan una protección suficiente en materia de responsabilidad civil equivalente al de las víctimas de daños causados (por bienes y servicios) sin que medie IA. Se trata de establecer un régimen análogo o equiparable a los supuestos de responsabilidad derivada del uso de la IA no cubiertos por la Directiva de 2024 de productos defectuosos. La cuestión de la carga de la prueba y las particularidades propias de la IA plantean problemas significativos para las normas de responsabilidad civil existentes, lo que se trataba de mitigar a través de esta propuesta de Directiva. Con este fin se buscaba de aligerar la carga de la prueba para el perjudicado, específicamente a través de las figuras de la exhibición de pruebas (art. 3) y de las presunciones refutables (art. 4).

77. Este apartado se ha convertido en un análisis de una propuesta de norma comunitaria que no llegará a ser. Por consiguiente, debe tomarse como una reflexión prospectiva de *lege ferenda*, que podría inspirar en su caso una posible futura propuesta revisada. El pasado 11 de febrero de 2025, la Comisión Europea anunció la retirada de su propuesta de Directiva sobre responsabilidad civil en inteligencia artificial. Esto supone un claro retroceso normativo en lo que se refiere a la protección de los "afectados" en este esté específico contexto, que se manifiesta cada vez más presente. Esta exclusión supone más que significativas consecuencias jurídicas —perjudiciales— para los eventuales perjudicados/víctimas de daños por uso IA, particularmente cuando los supuestos de responsabilidad no puedan encajar dentro de la categoría de "productos" (defectuosos) para poder tener un marco jurídico concreto y seguro para fundamentar sus pretensiones. Información de la retirada obtenida del *Programa de trabajo para 2025 de la Comisión*, titulado *Avanzar juntos: una Unión más audaz, más sencilla y más rápida,* presentado el pasado 11 de febrero (disponible en *https://commission.europa.eu/publications/2025-commission-work-programme-and-annexes_en)*. En el Anexo IV se retirará la propuesta de Directiva sobre responsabilidad civil en el ámbito de la IA. El motivo alegado es, una vez más, la falta de un acuerdo previsible, pero se especifica que la Comisión tiene intención de evaluar si presenta una propuesta revisada o explora un enfoque alternativo ante la necesidad de regulaciones que establezcan un marco claro de responsabilidad civil en sistemas de IA.

78. Texto disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=-CELEX:52022PC0496

Esta Directiva se aplicaría concretamente a demandas civiles de responsabilidad extracontractual por daños y perjuicios causados por sistemas de IA, cuando dichas demandas se interpongan en el marco de regímenes de responsabilidad por culpa o negligencia (lo que para el caso de las plataformas digitales vendría a complementar el régimen de responsabilidad que este entorno se establece en la DSA[79]). Nos centraremos en las principales novedades de presentaba la ahora malograda propuesta y que conllevaban significativas implicaciones (obligaciones) para para todos aquellos que participan en actividades relacionadas con sistemas de IA[80]. Para concluir, nos referiremos a su potencial aplicabilidad en concreto a las plataformas digitales y, en su caso, si resulta suficiente esta reglamentación —en los términos que estaban previstos— para los objetivos buscados.

22. Uno de los aspectos más significativos de la propuesta era la posible inversión de la carga de la prueba (Cdo. 14 y art. 1) en casos de daños relacionados con el uso de IA. Se aparta de esta forma de la aproximación que de esta cuestión se realiza en el Derecho tradicional, en el que el que reclama (el demandante[81]) debe demostrar que el producto o sistema de IA (en nuestro caso) causó el daño. Sin embargo, debido a la complejidad técnica de los sistemas de IA, la Comisión proponía que, en ciertos casos, la carga de la prueba recayese sobre el proveedor o desarrollador de la IA; en la medida que sean ellos los que tengan que demostrar que no hubo negligencia o que el sistema no presentó un fallo que causara el daño que se reclama. Esta inversión de la carga de la prueba solo se aplicaría en situaciones concretas: cuando el demandante tenga dificultades para obtener pruebas por la opacidad del sistema de IA (conocido como "caja negra"). Esta aproximación buscaba una mayor protección de las víctimas, al tiempo que impone una mayor responsabilidad a los desarrolladores/proveedores para garantizar que sus sistemas sean seguros y transparentes.

23. Otro aspecto relevante de la propuesta era el derecho de los demandantes a obtener acceso a pruebas relacionadas con los sistemas de IA en

79. Así lo reconoce el propio texto de la Propuesta, al indicar que "*la presente propuesta complementa otras vertientes de la política de IA de la Comisión basadas en requisitos preventivos normativos y de supervisión destinados directamente a evitar violaciones de los derechos fundamentales (como la discriminación), a saber: la Ley de IA, el Reglamento General de Protección de Datos, la Ley de Servicios Digitales y la legislación de la UE sobre no discriminación e igualdad de trato*", (…) y que "*no afecta a las normas vigentes* que *regulan las condiciones de responsabilidad establecidas por la Ley de Servicios Digitales*".

80. Generalmente operadores económicos, pero no en exclusiva, pues se prevén reglas incluso cuando su utilización esté fuera del ámbito profesional y se enmarque en actividades personales.

81. Típicamente el consumidor o usuario del producto o sistema.

litigios de responsabilidad (art. 3). La figura de la exhibición de pruebas permite a los tribunales nacionales ordenar la exhibición de pruebas pertinentes relativas a los sistemas de IA denominados de alto riego específico —de conformidad con el Reglamento IA— que se sospechen que hayan causado daños. Esta orden se dirige a los proveedores de sistemas de IA, a una persona sujeta a las obligaciones de promovedor o a un usuario de IA[82]. Ahora bien, este derecho de acceso no preveía como ilimitado. Así, para evitar abusos, la propuesta de Directiva preveía que se limitara a lo necesario y proporcional, para proteger los secretos comerciales (Cdo. 20). Para incentivar la cooperación del eventual demandando se introducía en la propuesta la "presunción de incumplimiento del deber de diligencia" del demandado cuando incumpla este requerimiento[83], si bien con el derecho de refutar tal presunción[84].

24. En lo que respecta a los daños causados por sistemas de IA, la propuesta pretendía proporcionar un fundamento eficaz para reclamar una indemnización en relación con la culpa consistente en el incumplimiento de un deber de diligencia en virtud del Derecho de la Unión o nacional. Así, se introduce en el art. 4 una presunción refutable de relación de causalidad en caso de culpa[85], que suponía que los tribunales nacionales presumirán, a efectos de la aplicación, a demandas por daños y perjuicios, de las normas de responsabilidad contenidas en el instrumento, el nexo causal entre la culpa del demandado y los resultados producidos por el sistema de IA o la no producción de resultados por parte del sistema de IA, cuando se cumpla una serie de requisitos. Lo que se busca con esto es facilitar a los demandantes la labor de probar la existencia del nexo causal entre el incumplimiento (de ese deber de diligencia exigido por noma UE o nacional) y la información de salida producida por el sistema de IA —o la no producción de una información de salida por parte del sistema de IA— que haya dado lugar a los daños en cuestión. Por ello se partía de una presunción refutable (*iuris tantum*)[86] de causalidad específica en relación con este nexo causal. El

82. Esta solicitud debería estar fundamentada en hechos y pruebas suficientes para poder acreditar la viabilidad de la eventual demanda de responsabilidad. Puede, en este sentido, establecerse más de un paralelismo con la figura del Derecho procesal civil español de la Diligencias preliminares que exigen acreditar un interés legítimo y una justa causa para su adopción (art. 258 en relación con las diligencias previstas en el art. 256 LEC).
83. A los efectos del art. 4 apartado 2 y 3.
84. *Vid*. art. 4, apartado 7.
85. Se trataba de una presunción refutable (*iuris tantum*), por lo que el demandado tiene la posibilidad de refutarla, en particular demostrando que su culpa no puede haber sido la causa del daño (considerando 30).
86. En el entendimiento de que esta presunción es la medida menos gravosa para dar respuesta a la necesidad de una indemnización justa para la víctima.

demandante debería demostrar la culpa del demandado con arreglo a las normas nacionales o de la Unión aplicables. Esta culpa podría determinarse, por ejemplo, por incumplimiento de un deber de diligencia en virtud de la Reglamento de la IA[87] —en general para todos los sistemas de IA, pero especialmente para los de alto riesgo—. El tribunal también podría presumir la culpa sobre la base del incumplimiento de una orden judicial de exhibición o conservación de pruebas con arreglo al art. 3, apdo. 5[88]. Ahora bien, solo procedía introducir una presunción de causalidad cuando pudiera considerarse probable que la culpa en cuestión hubiera influido en la información de salida del sistema de IA pertinente —o en la ausencia de la información de salida—, lo cual podría evaluarse en función de las circunstancias generales del caso. Al mismo tiempo, el demandante aún tendría que demostrar que el sistema de IA (es decir, su información de salida o la no producción de una información de salida) ha causado los daños. Asimismo, esta presunción (su alcance y condiciones) operaba o se modulaba en función del tipo de riesgo del sistema de IA de que se trate, calificado a la luz de la norma de referencia: el Reglamento IA, así como del tipo de demandado de que se trate. Este artículo, para establecer esta presunción, diferenciaba entre demandas interpuestas frente a proveedores de sistemas de IA de alto riesgo y aquellas interpuestas frente a usuarios de dichos sistemas (entre los que estarían los usuarios digitales de las plataformas digitales que publican y difunden a través de sus servicios contenidos generados por IA que puedan ser lesivos, así como las propias plataformas en línea que utilizan las IA para sus labores de moderación y recomendación de contenidos).

25. Cuando se trate de sistemas de IA de alto riesgo[89], los apartados 2 y 3 del art. 4 distinguían entre, por un lado, las demandas interpuestas contra el

87. Esto puede ponerse en relación con la eventual exigencia a las plataformas digitales (buscadores) de la adopción de medidas de etiquetado (del Reglamento IA) para distinguir claramente contenido generado por IA que se difunde a través de sus servicios. *Vid. infra* Apdo. III. 2.2. O de otras normas establecidas desde la Unión, como las que regulan el uso de la supervisión y la toma de decisiones automatizadas para el trabajo en plataformas o las que regulan el funcionamiento de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0496).

88. *Cuando un demandado incumpla la orden de un órgano jurisdiccional nacional en una demanda por daños y perjuicios de exhibir o conservar las pruebas que obran en su poder con arreglo a los apartados 1 o 2, el órgano jurisdiccional nacional presumirá el incumplimiento por parte del demandado de un deber de diligencia pertinente, en particular en las circunstancias a que se refiere el artículo 4, apartados 2 o 3, que las pruebas solicitadas estaban destinadas a probar a efectos de la correspondiente demanda por daños y perjuicios.*

89. Tal y como se definen en el Reglamento IA, según lo establecido en el Cap. III. Como son aquellos que afecten a derechos fundamentales (como pueden ser, por ejemplo,

proveedor o contra una persona sujeta a las obligaciones del proveedor (en virtud del Reglamento de IA) y, por otra parte, las demandas interpuestas contra el usuario de dichos sistemas. A este respecto, se siguen las disposiciones respectivas y las condiciones pertinentes del Reglamento IA[90]. En el caso de las demandas fundadas en el artículo 4, apartado 2 —frente al proveedor o equivalente—, el cumplimiento por parte de los demandados de las obligaciones enumeradas en dicho apartado debía evaluarse también a la luz del sistema de gestión de riesgos y sus resultados, esto es, las medidas de gestión de riesgos impuestas por el Reglamento IA. Para los sistemas de IA de alto riego, además, se establecía una excepción a la presunción de causalidad cuando el demandado pruebe que el perjudicado pudiera acceder razonablemente a pruebas y conocimientos específicos suficientes que permitan acreditar adecuadamente el nexo causal (art. 4, apartado 4); lo que estaba vinculado con la necesaria cooperación en la práctica de diligencias de exhibición del art. 3 o la garantía de transparencia del sistema[91].

En el caso de los sistemas de IA de riesgo no elevado, de conformidad con el artículo 4, apartado 5, la presunción estaba sujeta al criterio del juzgador, que determinaría su aplicabilidad o no sobre la base de un juicio de dificultad probatoria del nexo causal por el demandante. Estas dificultades deberían evaluarse no sólo a la luz de las características particulares de determinados sistemas de IA (como son la autonomía y la opacidad, que hacen muy difícil en la práctica la explicación del funcionamiento interno del sistema de IA —lo que afecta negativamente a la capacidad del demandante para señalar el nexo causal entre la culpa del demandado y la información de salida de IA, o falta de ésta—), sino también de las circunstancias del propio demandante[92]. Para aquellos supuestos en los que el demandado utilice el sistema de IA en el transcurso de una actividad personal y no profesional[93], el artículo 4, apartado 6, establecía que la presunción de causalidad solo debe

---

aquellos que contribuyan a la desinformación con el objeto de incidir en procesos democráticos).

90. Cuya inobservancia supone el incumplimiento de la diligencia debida como requisito o condición necesaria para el cumplimiento de la presunción de causalidad.

91. Esta posibilidad puede incentivar a los demandados a cumplir sus obligaciones de exhibición, las medidas establecidas por el Reglamento IA para garantizar un alto nivel de transparencia de la IA o los requisitos de documentación y registro.

92. Sobre la base de estos criterios, y en la medida que no se concreten legalmente por los Estados miembros en su transposición, será el desarrollo jurisprudencial (TJUE) el que permita establecer los parámetros de aplicación razonables en función de las circunstancias del caso concreto.

93. Típicamente las circunstancias que concurren en los usuarios digitales de las plataformas en línea.

aplicarse si el demandado ha interferido sustancialmente en las condiciones de funcionamiento del sistema de IA o si el demandado tenía la obligación y estaba en condiciones de determinar las condiciones de funcionamiento del sistema de IA y no lo hizo. Esta condición se justificaba por la necesidad de ponderar los intereses de los perjudicados y de los usuarios no profesionales, eximiendo de la aplicación de la presunción de causalidad aquellos casos en que los usuarios no profesionales no incrementen el riesgo a través de su comportamiento. En todo caso, al demandado le asistía el derecho a refutar la presunción de causalidad basada en el art. 4, apdo. 1 (de conformidad con su apdo. 7).

Estas normas vinculaban la presunción de causalidad (por culpa) al cumplimiento de las obligaciones de diligencia debida que las distintas normas (de la UE[94] o nacionales) articulan para todos aquellos que participan en actividades relacionadas con sistemas de IA; por lo que constituirían sin duda un incentivo adicional para el cumplimiento de todas las obligaciones[95] previstas en este ámbito, para evitar incurrir en eventuales responsabilidades. Obligaciones todas ellas dirigidas a asegurar que todos estos agentes vinculados implementen medidas adecuadas de diligencia, transparencia y supervisión para minimizar los riesgos de la IA y garantizar la protección de los derechos de los ciudadanos[96].

---

94. En esta Directiva, en el Reglamento de IA, el Reglamento General de Protección de Datos, la DSA, etc. Como son las obligaciones vinculadas a la transparencia que tienen como objetivo permitir la trazabilidad y aplicabilidad de las decisiones tomadas por los sistemas automatizados. Como así se recoge en el art. 3 de la propuesta que implica que las empresas que desarrollen o utilicen sistemas de IA, especialmente aquellos de alto riesgo, proporcionen acceso a información clave sobre el diseño, desarrollo y funcionamiento de los sistemas de IA.

95. Incluso aquellas que no se recogen específicamente como tales, pero que del texto se deriva la importancia de "adelantarse" a esta necesidad. Así, aunque no aparece especificado en ningún artículo de la propuesta de Directiva, las empresas que trabajen con sistemas de IA de alto riesgo deben considerar la contratación de seguros de responsabilidad civil para protegerse frente a posibles reclamaciones por daños. Este aspecto surge como consecuencia de las obligaciones impuestas en los artículos mencionados y la naturaleza de los riesgos asociados a estos sistemas.

96. La propuesta de Directiva trataba de ofrecer un marco legal moderno que equilibre la innovación tecnológica con la responsabilidad y la protección de los derechos fundamentales de los ciudadanos, completando el marco jurídico ya existente en este sentido, ya que "*complementa otras vertientes de la política de IA de la Comisión basadas en requisitos preventivos normativos y de supervisión destinados directamente a evitar violaciones de los derechos fundamentales (como la discriminación), a saber: la Ley de IA, el Reglamento General de Protección de Datos, la Ley de Servicios Digitales y la legislación de la UE sobre no discriminación e igualdad de trato*". https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0496

26. A través de figura de las presunciones refutables prevista en esta propuesta, se trataba de buscar un régimen de responsabilidad tendente a la objetivación, propio de los sistemas de protección de consumidores y usuarios frente a daños causados por bienes y servicios, y que hace recaen sobre el prestador del servicio o suministrador del bien la carga de la prueba de empleado de diligencia adecuada de conformidad con la naturaleza de los bienes y la prestación de los servicios de los que se traten; pero se mantenía la necesidad de probar el nexo causal por parte del demandante perjudicado. Consecuentemente, esta previsión expresa de una presunción (aun refutable) de causalidad en los términos expuestos, era sin duda un avance y un beneficio significativo para los consumidores y usuarios que puedan verse perjudicados por sistemas de IA (especialmente de alto riesgo) para exigir responsabilidades; pero no se trataba de una responsabilidad objetiva en sentido estricto[97]. De hecho, la propuesta preveía una revisión de la Directiva por la Comisión después de la finalización del período de transposición, tras evaluar su funcionamiento[98], para examinar si fuera necesario adoptar normas de responsabilidad objetiva para demandas contra los operadores de determinados sistemas de IA[99].

27. La aplicabilidad de esta normativa propuesta al objeto de estudio, demandas civiles responsabilidad por daños causados por supuestos de informaciones falsas (desinformación) creadas o tratadas por IA, publicadas en plataformas digitales, parece posible. Según esta propuesta se aplicaría a las demandas de responsabilidad civil extracontractual subjetiva (basada en la culpa) en aquellos casos en que los daños y perjuicios son causados por un sistema de IA después de su entrada en aplicación —tras el período de transposición—. Los eventuales demandados —posibles responsables—, como destinatarios de las disposiciones recogidas, no solo se limitaría a los proveedores de sistemas de IA sino también personas que respondan como tales de conformidad con el Reglamento IA[100], así como usuarios del sistema de IA[101]. Así pues, dentro de la figura del usuario del sistema de IA (en los

97. Dadas las excepciones a la operatividad de la presunción, que devuelve al demandante la responsabilidad de la carga de la prueba, además del carácter refutatorio de la presunción (garantizando el derecho del demandado de desvirtuarla), unido al hecho de que se mantiene la obligación del demandante de probar el nexo causal entre el daño y ese comportamiento no diligente del eventual responsable.
98. *Vid*. art. 5.
99. *Vid*. Considerando 31.
100. Al remitir su art. 2.3 la definición de proveedor a la recogida en el Reglamento IA (art. 3. 2)
101. En los términos establecidos por el Reglamento IA (art. 3.4), igualmente por remisión expresa de la Directiva (art. 2.4).

supuestos de referencia) podría encajar el usuario de la plataforma digital que utiliza sus servicios para publicitar la información falsa creada por IA generativa, o la propia plataforma digital que recurre a este tipo de sistemas de IA para realizar su función de control (proactivo) de contenidos al que está obligado por la DSA en su consideración de muy grande plataforma (vinculado a la necesaria evaluación de riesgos sistémicos y adopción de medidas para su mitigación). Ahora bien, al no concebirse los sistemas de IA generativa o en general los modelos fundacionales como sistemas de alto riesgo *per sé*—como se ha expuesto anteriormente—, la aplicación de la norma del art. 4.1, relativa a la presunción de "parte"[102] del nexo causal quedaría al arbitrio judicial cuando considere que es "excesivamente difícil" para la víctima probarla (art. 4.5). A ello se une el hecho de que en la mayoría de estos casos el daño ocasionado suele ser un daño no material, es decir, un daño moral; sin que exista un marco normativo armonizado en relación con este tipo de daños dentro de la UE[103]. En consecuencia, para estos casos nos encontramos con una regulación sectorial en los ordenamientos jurídicos nacionales, pero además los criterios jurisprudenciales respecto de su compensación son muy dispares entre los Estados miembros de la UE.

28. En definitiva, la propuesta analizada constituiría un avance importante en la reglamentación de la implantación de la IA dentro de la UE. El texto propuesto aumentaba la seguridad jurídica y facilitaba el resarcimiento de los daños eventualmente ocasionados por el uso de esta tecnología, aunque planteaba ciertas cuestiones para la tutela de los intereses del eventual perjudicado en el ámbito de la responsabilidad por IA generativa que podrían mejorarse. Especialmente esta afirmación es debida a su consideración como sistemas de riesgo moderado, lo que reduce la operatividad de la presunción (*iuris tantum*) de causalidad en caso de culpa dejándolo a la discrecionalidad del juzgador; lo que unido al hecho de que en estos casos se trata de daños no materiales (morales) no armonizados dentro de la UE, no parece una respuesta muy favorable para el presunto perjudicado. En cualquier caso, habrá que estar a la publicación del texto definitivo de la Directiva, si es que se retoma esta iniciativa, así como su efectiva implementación por las respectivas legislaciones nacionales de los Estados miembros[104], para evaluar su efectividad y adecuación a los objetivos marcados. No puede olvidarse

102. En favor del perjudicado demandante.
103. *Vid*. C. WENDEHORST, "Study on Safety and Liability Related Aspects of Software. Shaping Europe´s digital future", *EU Commission*, 2021. Study on Safety and Liability Related Aspects of Software | Shaping Europe's digital future, apdo. 4.1.6.2 Physical risks.
104. *Vid.* art. 7.

que se trata de una tecnología que progresa de manera exponencial en corto período de tiempo, con unas posibilidades infinitas de desarrollo (lo que juega en contra de una reglamentación ajustada a la realidad vigente), que debe regularse de manera conciliadora con la protección de los derechos fundamentales y la garantía de indemnidad ante cualquier daño.

3. EL USO DE LA IA PARA LA CREACIÓN DE CONTENIDOS EN LA DSA

29. La vinculación de la IA con las actividades de los prestadores de servicios en línea cubiertos por la DSA se articula bien por su recurso por los propios operadores digitales, bien por su utilización por los usuarios digitales de estos espacios para la creación de contenidos que se publican y diseminan a través de estos servicios en línea. En el primero de los casos se trata de sistemas de IA en sentido amplio, que se configuran en términos generales como sistemas algorítmicos que permiten gestionar automáticamente grandes cantidades de datos para tomar decisiones automatizadas de manera rápida y eficaz[105]. En este sentido, se constata la utilización por los grandes prestadores de servicios digitales de los sistemas de IA para realizar la labor de moderación y control (proactiva) de contenidos potencialmente lesivos —o que conculquen sus condiciones generales— publicados o difundidos a través de sus servicios por los usuarios, para no incurrir en responsabilidad vinculada al deber de diligencia en este sentido impuesta por la DSA. A esta actividad ha de añadirse la conocida como labor de curación de contenidos realizada por estos agentes (para personalizar y recomendar contenidos a los usuarios[106]), igualmente con el recurso típico a los mecanismos automatizados mediante IA[107]. Ambas actividades vinculadas con el uso de la IA estarían cubiertas por la DSA y, en consecuencia, su desarrollo debe realizarse con seguimiento de las disposiciones impuestas por este instrumento para los prestadores de servicios digitales que operen dentro de la UE[108].

---

105. En profundidad lo veremos en los Apdos. III. 1.2 y 1.3.
106. Su utilización puede tener efectos negativos no deseados como es la creación de lo que se conocen como "burbujas de filtro" que pueden aislar al usuario de información diversa y esto, también puede conducir a esa desinformación no deseada. *Vid. infra* nota 175.
107. *Vid.* J. J., CASTELLÓ PASTOR, "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", Vol. 17, n.º 1 (marzo 2025), *CDT,* pp. 308-328.
108. En especial, en la lucha contra la desinformación dentro de la UE mediante uso de sus servicios digitales. *Vid. infra* Apdo. III.

Es en la segunda de las aproximaciones, la relacionada con la actividad de los usuarios digitales de los prestadores de servicios en línea de intermediación, en la que interviene la IA generativa, respecto de la cual se plantea su regulación dentro de la DSA en relación con los agentes implicados[109]. En el ámbito que nos ocupa, con los sistemas o modelos de IA generativa se pueden crear contenidos falsos (o manipulación de información en principio real) que pueden ser complicados de detectar por la redacción y estilo utilizado para su creación[110]. Con estos elementos cabe plantearse si la eventual responsabilidad derivada de ese control defectuoso, o no control de contenidos generados por la IA que se impone en la DSA, puede exigirse no solo a los muy grandes prestadores de servicios digitales (destinatarios naturales de la norma) sino también a los responsables del sistema de IA generativo utilizado. Es necesario, en primer lugar, plantearse si la DSA constituye marco jurídico aplicable a estos operadores económicos. El análisis de los ámbitos de aplicación de la DSA es necesario para dar la respuesta a esta cuestión. Partimos del hecho de que la eventual responsabilidad por contenidos lesivos o no deseados (como es la información falsa, *fake news*, bulos…, entre otros supuestos), están dentro del ámbito de actuación de la DSA, cuando esta información (generada por IA) es publicada y difundida por usuarios reales o falsos mediante los servicios en línea de prestadores digitales que operan dentro de la UE[111].

30. Entre las implicaciones que la DSA impone en este contexto a los considerados como prestadores de servicios digitales cubiertos, destaca la obligación de incorporar un mecanismo de notificaciones a través del cual los usuarios pueden denunciar contenido ilícito (art. 3 letra h DSA) que debe ser revisado por ellas y, en su caso, eliminado de la plataforma si verdadera-

109. Sobre esta cuestión en particular, *vid*. S. NAVAS NAVARRO, "Moderación de contenido e Inteligencia artificial generativa", *Derecho y digitalización empresarial. Reflexiones sobre el impacto de la digitalización en el Derecho que regula la actividad empresarial*. https://webs.uab.cat/derecho-y-digitalizacion-empresarial/2023/07/12/moderacion-de-contenido-e-inteligencia-artificial-generativa/

110. En este sentido, es fácil encontrar en *YouTube* tutoriales de cómo realizarlo.

111. Partiendo de su ámbito de aplicación espacial, la DSA se aplica a aquellos servicios digitales ofrecidos a usuarios en la UE, independientemente de dónde se encuentre el establecimiento, sede o domicilio del proveedor del servicio en línea. *Vid*. Art. 2.1, 3 letra d y e DSA. Sobre el alcance territorial de la DSA, véase S. FELIU ÁLVAREZ SOTOMAYOR, "Ámbito territorial y aplicación del principio del control en origen en el Reglamento UE de servicios digitales", en AA.VV. *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2024, pp. 41-64; S. BERNASCONI, "Il ruolo del diritto internazionale privato e processuale nell'attuazione del 'pacchetto sui mercati e servizi digitali' (DMA&DSA)", *RDIPP*, 4/2024, pp. 1184-1307.

mente es una información ilícita (art. 16 DSA: *notice-and-action-system*). Para las consideradas como muy grandes plataformas —y motores de búsqueda— las obligaciones se incrementan, ya que además deben establecer un sistema interno de gestión de reclamaciones (art. 20 DSA) y un sistema de resolución extrajudicial de conflictos (art. 21 DSA). A mayor abundamiento, si se constata por el prestador de servicios que un usuario es reincidente en publicar/difundir contenido ilícito (generado o no con intervención de la IA) con su intermediación, pueden suspender sus servicios para esa cuenta (art. 23 DSA). Una de las vías previstas por la DSA para el control de esos contenidos potencialmente problemáticos se articula a través de los alertadores fiables[112]; además de otros mecanismos que puedan adoptarse por los operadores vinculados. En este sentido, el contenido calificado como problemático por alertadores fiables debe ser priorizado y se debe decidir sin dilación por la plataforma si se retira o no (art. 22 DSA). En lo que respecta a las declaradas como muy grandes plataformas, estas deberán implementar un mecanismo de respuesta a las crisis y someterse a auditorías independientes (arts. 36-37 DSA); además de otras obligaciones sustantivas que pueden vincularse en este contexto (como evaluación de riesgos sistémicos y adopción de medidas para su mitigación)[113].

31. Es esencial determinar si entre los destinatarios de estas obligaciones están los responsables de los sistemas o modelos de IA utilizados para crear ese contenido ofensivo que se difunde en estas redes. La DSA establece que se aplica a los proveedores de servicios digitales de intermediación, también denominados "servicios intermediarios"[114]. Qué constituye esos servicios es esencial para poder resolver esta cuestión. Estos se enumeran en el art. 3 letra g de la DSA como servicios de mera transmisión, de memoria caché y de alojamiento de datos (como serían las redes sociales o plataformas en línea y motores de búsqueda)[115]. La IA generativa —o más ampliamente los modelos fundacionales— no entran dentro de ninguna de estas categorías referidas en atención a la descripción que de cada uno de estos servicios

112. Entre otras vías, siendo las que interviene la IA para esa labor en la que nos centraremos en el siguiente apartado por el objeto de estudio.
113. . *Vid. infra* Ap. III.
114. Arts. 2.1 y 2.2, DSA.
115. Sobre esta última opción de servicios de intermediación, véase considerando 28 DSA. Respecto de la responsabilidad que sobre este tipo de prestadores de servicios de intermediación recae a la luz del art. 14 DSA, véase Comisión Europea: Dirección General de Redes de Comunicación, Contenido y Tecnología, J. HOBOKEN, J. QUINTAIS, J. POORT y N. EIJK, "*Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report*", *Oficina de Publicaciones*, 2019, https://data.europa.eu/doi/10.2759/284542

de intermediación se realiza por la DSA. Cabría platearse si los sistemas de IA son prestadores de servicios digitales de intermediación respecto de sus usuarios y los contenidos generados a través de estos sistemas o modelos, pero no es así. Los usuarios de los modelos de IA generativos de contenidos (como es el *ChatGPT*) no generan ellos el contenido, sino que solicitan información a la IA. Es el propio sistema (*ChatGPT* en el ejemplo) el que genera el contenido en función de las instrucciones (o *prompts*) que se le facilitan; no es el usuario el que genera ese contenido, lo que sería necesario para que le fuera de aplicación a los responsables de esa IA generativa la DSA con las referidas implicaciones (obligaciones sustantivas) previstas como prestadores intermediaros. En consecuencia, debe concluirse que la norma europea no se aplica a estos sistemas de IA[116]. De esta suerte, excluida la aplicabilidad de la DSA[117], para determinar la eventual responsabilidad en este ámbito por los sistemas o modelos de IA a sus responsables, habrá de acudirse a otras normas potencialmente operativas. Entre ellas, por ejemplo, aquellas sobre responsabilidad civil extracontractual (donde estaría en su momento una eventual Directiva sobre responsabilidad derivada del uso de la IA o la vigente Directiva de productos defectuoso en aquello cubierto) o las relacionadas con los discursos de odio, libertad de expresión o protección de derechos de la personalidad, reglamentados por Derechos nacionales de los Estados miembros[118]; además, por su puesto, de las disposiciones contenidas en el Reglamento IA.

32. Sí cabe la aplicación de la DSA de manera indirecta a los sistemas y modelos de IA generativa cuando es un usuario real del sistema —o incluso un *bot*— el que publica y difunde el contenido generado por la IA (información no veraz o manipulada perseguible) a través de plataformas digitales cubiertas por la DSA. En estos casos, cuando se haya producido difusión al público[119] de este contenido potencialmente ilícito —no deseado— se alzan las obligaciones recogidas por la DSA para las plataformas digitales —como prestador de servicios de intermediación— relativas al moderación y control de riesgos sistémicos ya anticipadas. Esta exigencia de difusión al público

116. En este sentido se manifiesta, S. NAVAS NAVARRO, "Moderación de contenido e Inteligencia artificial generativa", *ob. cit.*

117. No se aplicarán los diferentes mecanismos que la DSA ha establecido en caso de contenido ilícito y discursos del odio.

118. O de Derecho de la Unión en su caso. Así, si se procede por el sistema de datos personales de las víctimas del daño, operara el art. 82, apdo. 1.º del RGPD.

119. Que debe diferenciarse de los supuestos en los que la publicación de la información no supone difusión al público; por ejemplo cuando se hace como "mensaje privado", de manera que restringe el acceso a este contenido a uno o varios usuarios (o grupos de usuarios). *Vid.* a este respecto, Considerando 14 DSA.

supone que quedan cubiertas aquellos supuestos en los que la información lesiva se publican en plataformas que diseminan la información al público, en particular, aquellas muy grandes o de muy gran tamaño [120] (como son las redes sociales *Facebook, Instagram, YouTube* o *X*). De esta forma, si la información se distribuye a través de grupos de *WhatsApp, Telegram* u otras vías de distribución selectiva y restrictiva —entornos en los que prolifera este tipo de contenido problemático— quedan fuera del ámbito de aplicación de la DSA [121]. En definitiva, y en consecuencia, para poder aplicar la DSA a los contenidos generados por la IA, estos deben ser publicados en las plataformas online que podrían considerarse como "clásicas" [122]. Habrá que estar atentos a la evolución del uso de los sistemas de IA en relación con las destinatarios naturales de las disposiciones de la DSA; entendiendo que a medida en que se vayan integrando estos sistemas en los motores de búsqueda será más evidente la aplicación de la DSA a los contenidos generados.

33. Como conclusión, quizá sería conveniente modificar el ámbito de aplicación subjetivo de la DSA, para introducir todos los supuestos de IA y equiparar el contenido creado por sistemas de IA generativa a los contenidos generados por los usuarios de las plataformas digitales (que las utilizan para su difusión), a los efectos de que puedan aplicarse las medidas y mecanismos de control del contenido ilícito, no solo a los prestadores de servicios de intermediación en línea, sino también a los responsables de los sistemas y modelos de IA utilizados para realizar esta actividad ilícita.

III. MECANISMOS DE LUCHA CONTRA LA DESINFORMACIÓN DENTRO DE LA UE EN EL USO DE LOS SERVICIOS DIGITALES

34. Revisado el marco jurídico potencialmente aplicable para despejar eventuales responsabilidades para los supuestos en los que intervenga tecnología IA, vamos a centrarnos específicamente en los mecanismos de lucha contra la desinformación previstos específicamente en relación con las plataformas digitales (incluidos buscadores) que operan dentro del mercado interior, como principal vehículo para la publicación (difusión pública) de

120. Art. 19.2 DSA.

121. *Vid.* F. WILMAN, "The Digital Services Act (DSA): An Overview (16 de diciembre de 2022)". *Comisión Europea.* Disponible en SSRN: https://ssrn.com/abstract=4304586 (fecha consulta: 11 noviembre 2024)

122. *Cfr.* P. HACKER, A. ENGEL, M. MAUER, "Regulating ChatGPT and other Large Generative AI Models", *working paper*, disponible en https://arxiv.org/pdf/2302.02337 (Fecha de la consulta: 11 noviembre de 2024 2023), pp. 1-31, en esp. p. 16.

los contenidos no reales que participan de este ilícito objetivo[123]. En este contexto, la DSA se alza como el principal instrumento para el control de los eventuales contenidos ilícitos o no deseables publicados o difundidos mediante los servicios digitales. Este control se realiza mediante la articulación de una serie de obligaciones sustantivas (de diligencia debida) impuestas particularmente a los grandes prestadores de servicios digitales de intermediación que almacenen estos datos (muy grandes plataformas digitales) que inciden directamente en su régimen de responsabilidad, vinculando éste a su cumplimiento[124]. En este ámbito, como ya se ha referido, en cumplimiento de estas medidas las grandes plataformas recurren típicamente al uso de sistemas de IA (mecanismos automatizados). Cuando estos agentes digitales sean de muy gran tamaño, la DSA contiene disposiciones de obligada observancia en materia de información, transparencia y rendición de cuentas para mitigar los riesgos sistémicos en línea, enfocándose especialmente en el uso de la IA —cuestión distinta es si estas obligaciones son suficientes o resultan eficaces—. Asimismo, en los últimos tiempos se ha señalado incluso que ciertas plataformas digitales no solo contribuyen sino que fomentan la difusión de información falsa (bulos, *fake news*, determinada propaganda…), fundamentalmente a través de la curación de contenidos, con el objeto de incidir en la decisión de los usuarios de estas redes en distintos procesos decisorios (fundamentalmente de índole electoral)[125]. Como complemento de la DSA, y junto con los códigos de conducta y de buenas prácticas presentados por la Comisión Europea en la lucha contra los contenidos no deseados en general[126], específicamente desde 2018 existe

123. No así el contenido, que no tiene por qué ser ilícito, pero sí las consecuencias, al ser información errónea, falsa o inexacta que causa desinformación. Esta desinformación puede ser buscada, cuando es el usuario real o a través de perfiles falsos el que lo publica y difunde a través de la plataforma; pero también no buscada, cuando es consecuencia del uso de la IA (métodos automatizados) por la propia plataforma en el ejercicio de su labor de control (proactivo) de contenidos o incluso de curación.

124. *Vid.* C.I. CORDERO ÁLVAREZ, "El régimen de responsabilidad de las plataformas online en la DSA…", *ob. cit.*, Apdo. III.3.

125. Lo que ha provocado que se insten institucionalmente distintos procesos de investigación frente a muy conocidas redes sociales. La Comisión Europea abrió, el pasado 18 de diciembre de 2023, un proceso formal para investigar presuntos incumplimientos de la DSA por parte de *X*, la antigua *Twitter*, entre los que se encontraría la falta de diligencia de la empresa de Elon Musk contra la desinformación y los contenidos ilegales. Toda la información sobre este procedimiento, las tapas y siguientes pasos en https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6709 (consultado 15 noviembre de 2024). Y no es la única plataforma que está siendo investigada dentro de la UE por esta razón (y otras que suponen el incumplimiento de la DSA). Este es el caso de *TikTok* (*vid.* Apdo. III.2.2.).

126. *Vid*. nota n.º 152.

un código de buenas prácticas en materia de desinformación (suscrito por 34 plataformas digitales) que se ha visto reforzado en 2022. A esta última iniciativa se une a serie de Directrices presentadas por la Comisión en el año 2024, para las plataformas digitales, a los efectos de coadyuvar en la lucha contra la desinformación —y manipulación de información—, en particular, cuando estas operaciones de desinformación se enmarcan dentro de procesos electorales.

1. OBLIGACIONES SUSTANTIVAS PARA LOS GRANDES PRESTADORES DE LA DSA Y EL RECURSO A LA IA PARA SU CUMPLIMIENTO

35. Son varias las obligaciones sustantivas, vinculadas a la diligencia debida, que la DSA impone a las declaradas como muy grandes plataformas digitales y motores de búsqueda conectadas con el objeto de estudio. Como punto de partida, de conformidad con el artículo 34, apartados 1 y 2, y el artículo 35, apartado 1, las plataformas en línea de muy gran tamaño están obligadas a detectar, analizar y evaluar con diligencia cualquier riesgo sistémico en la Unión derivado del diseño o el funcionamiento de su servicio y sus sistemas conexos, o del uso que se haga de sus servicios. En la medida que la gestión de riesgos sistémicos no solo exige su detección y evaluación, sino su mitigación mediante a adopción de medidas razonables, proporcionadas y efectivas, frente en general a contenido ilícitos, y en especial para "cualquier efecto negativo real o previsible en el discurso cívico y los procesos electorales"[127], esto también condiciona sus actuaciones para evitar responsabilidades. A este respecto, cabe destacar los artículos 9, 10, 16 y 22 de la DSA sobre contenidos ilícitos, que comprenden las órdenes de actuar contra este tipo de contenidos y de proporcionar información, así como los mecanismos de notificación y acción y la disposición sobre alertadores fiables. En el ámbito objeto de estudio, de conformidad con este instrumento europeo, hay otros requisitos que les son exigibles a las grandes plataformas y buscadores por operar dentro de la UE (en especial si se vincula la desinformación con procesos electorales). Estas obligaciones incluyen, entre otras, las contenidas en los arts. 14 y 17 (sobre las condiciones y declaración de motivos), los arts. 27 y 38 (sobre los sistemas de recomendación), los arts. 36 y 48 (sobre los mecanismos y protocolos de respuesta a las crisis), los artículos 15, 24, 37 y 42 (sobre la transparencia y las auditorías independientes), los artículos 26 y 39 (sobre la transparencia de la publicidad en línea) y el artículo 40 (sobre el acceso a los datos y el control).

127. Artículo 34(1)(c) de la DSA.

Al realizar evaluaciones de riesgos se deben tener en cuenta varios factores que influyen en los riesgos sistémicos, tales como los sistemas de recomendación, los sistemas de publicidad o la manipulación intencionada del servicio (por ejemplo, mediante el uso no auténtico o la explotación automatizada del servicio, así como la amplificación y la difusión potencialmente rápida y amplia de contenidos ilícitos y de información incompatible con sus condiciones generales o términos de uso). De esta suerte, las plataformas en línea de muy gran tamaño están obligadas a establecer medidas de mitigación razonables, proporcionadas y eficaces, adaptadas a los riesgos sistémicos concretos detectados. En estos casos, según el artículo 16, apartados 5 y 6, estos operadores digitales deben notificar sin demora indebida la decisión de moderación de contenidos a las personas físicas o entidades, facilitando información sobre las posibilidades de reparación en relación con tal decisión. Deben adoptar esas decisiones de manera oportuna, diligente, no arbitraria y objetiva. Asimismo, de acuerdo con el artículo 25, apartado 1, los prestadores de plataformas en línea no deben diseñar, organizar o gestionar sus interfaces en línea de manera que engañen o manipulen a sus usuarios, o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas. El artículo 39 obliga a las plataformas en línea de muy gran tamaño a compilar y hacer público, a través de una herramienta consultable y fiable, un repositorio que contenga anuncios en sus plataformas, hasta un año después de la presentación del anuncio por última vez, de manera que la información sea exacta y completa. Por último, a la luz del artículo 40, apartado 12, las plataformas en línea de muy gran tamaño deben facilitar a los investigadores un acceso efectivo a los datos de las plataformas. El cumplimiento de estas obligaciones puede ser objeto de investigación por parte de las autoridades nacionales y de la propia Comisión Europea con significativas consecuencias económicas[128].

36. Como punto de partida es necesario indicar que la DSA[129] no impone explícitamente la obligación a las plataformas en línea y motores de búsqueda de moderación de los contenidos nocivos e ilícitos, aunque esta sea la práctica de estos prestadores de servicios desde hace años. De hecho, se esta-

128. A los principales procedimientos formales de investigación incoados por la Comisión frente a las principales redes sociales que opera en la UE, se dedicará el Apartado III.2.1.

129. Ni tampoco previamente la DCE. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico, DCE).

blece expresamente la inexistencia de obligación general de monitorización o de búsqueda activa de hechos para estos operadores digitales (art. 8 DSA)[130] —aunque sí bien es cierto que otras recientes legislaciones sectoriales en el ámbito del Derecho de la Unión sí establecen este requerimiento[131]—. Las actividades voluntarias de moderación contenidos —e incluso de curación, como veremos posteriormente— se enmarcarían dentro de la necesidad de cumplir con las obligaciones de diligencia debida para crear un entorno en línea transparente y seguro que se imponen por la DSA a los prestadores de servicios de intermediación (Cap. III), y a cuyo cumplimiento se vincula en última instancia su régimen de responsabilidad; en particular, en relación con las obligaciones adicionales previstas para las muy grandes plataformas en línea y motores de búsqueda, en relación con el control de riesgos sistémicos vinculados a sus servicios[132]. Asimismo, la implementación de estos mecanismos voluntarios (proactivos) para detectar, identificar y retirar contenidos ilícitos, o inhabilitar el acceso a los mismos desde sus servicios se fomentan por el legislador europeo, en la medida en que no perderán su inmunidad si estas investigaciones voluntarias se llevan a cabo de buena fe y con diligencia (art. 7 DSA).

37. Como ya se refirió al abordar el planteamiento de este trabajo, hay varios aspectos clave en el uso de la IA por parte de las grandes plataformas en línea y motores de búsqueda que pueden focalizarse dentro de esa labor de luchar contra la desinformación como uno de los riesgos sistémicos indicados por las instituciones europeas, y que estos agentes deben evaluar y mitigar como obligaciones (sustantivas) impuestas por la DSA, si no quieren incurrir en responsabilidad[133]. En particular, en la práctica se constata el recurso general de la IA por estos operadores para moderar y curar contenidos publicados y difundidos a través de sus servicios digitales de intermediación (para la detección automática de contenidos potencialmente ilegales y otras medidas proactivas). Las grandes plataformas digitales, así como los motores de búsqueda, utilizan de manera generalizada sistemas de IA para moderar contenidos no deseados: para detectar y eliminar rápi-

130. Esta obligación sería contraria al artículo 15 DCE,

131. Este es el caso del artículo 17 de la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. DO L 130 de 17.5.2019, p. 92/125.

132. Obligaciones adicionales de gestión de riesgos sistémicos para prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño (Secc. 5, arts. 33-44)

133. *Vid.* C.I. CORDERO ÁLVAREZ, "El régimen de responsabilidad de las plataformas online…", *ob. cit.*

damente (de entre el ingente volumen de datos) el material ilícito o que viole las normas internas de la plataforma[134]. Las decisiones de moderación que se realizan, en un número elevado de casos, se hacen mediante sistemas completamente automatizados[135]. La razón es sencilla, la moderación automatizada permite realizar esta labor frente al enorme volumen de información y a la velocidad de creación de contenidos en internet —lo que es inviable mediante una revisión exclusivamente humana—. Esto puede ser peligroso si se tiene en cuenta los potenciales fallos en los algoritmos (que funcionan generalmente por probabilidad), lo que conduce en supuestos a limitar y borrar publicaciones que no son ilícitas, que no vulneran derechos

134. No obstante, se trata en términos generales de una aplicación de la IA en sentido amplio, esencialmente centrada en la automatización de las operaciones (no de carácter generativo). En este sentido, se manifiesta T. GILLESPIE, precisando que aunque algunas plataformas sí utilizan técnicas de aprendizaje automático para identificar nuevos contenidos no admisibles (casos de acoso, discursos de odio o pornografía), la mayoría de operadores realiza esta operación mediante comparación de patrones, esto es, se limitan a comparar el nuevo contenido con una lista negra de ejemplos ya conocidos elaborada previamente. Esto es claramente un supuesto de automatización, y solo de IA si se toma esta desde una definición lo más amplia posible. "Content Moderation, AI, and the Question of Scale", *Big Data & Society*, 2020, vol. 7, núm. 2, en esp. p. 3 (https://journals.sagepub.com/doi/epub/10.1177/2053951720943234). Un estudio de las herramientas de aprendizaje automático predictivo y de comparación de *hash* automatizadas (como *sistemas de moderación algorítmica*) para llevar a cabo la moderación de contenido a gran escala por parte de las principales plataformas para el contenido generado por los usuarios, en R. GORWA, R.BINNS y C. KATZENBACH, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance", *Big Data & Society*, febrero 2020 (https://journals.sagepub.com/doi/full/10.1177/2053951719897945)

135. Se constata, por la información remitida por las propias plataformas y motores de búsqueda a la Comisión Europea que, en promedio, estos operadores para la labor de moderación de contenidos, denuncias y restricciones de visibilidad de contenidos en la red, alrededor del 50% de estas decisiones se realizan a través métodos completamente automatizados (sobre la base de 106 plataformas activas). Información obtenida de la página web de la Comisión Europea "DSA Transparency Database" (https://transparency.dsa.ec.europa.eu consultada a fecha 27/12/2024). Aunque hay operadores que superan con mucho este porcentaje. En este sentido, llama la atención los datos facilitados por la plataforma *Youtube,* sobre el último trimestre 2023 (según consta en la página de la Comisión Europea "DSA Transparency Database"): eliminó más de 8.565.644 vídeos por medio de detección automática y el 99,6 % de los 1.197.687.868 comentarios retirados por esta plataforma fueron igualmente por detección automática. Un análisis pormenorizado sobre datos de utilización de sistemas automatizados para toma de decisiones por los grandes gigantes tecnológicos que operan en la UE, en cumplimiento de las obligaciones impuestas por la DSA, puede verse en J. J. CASTELLÓ PASTOR, "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda…", *ob. cit.* Apdo. I.

fundamentales, limitando libertades fundamentales de los usuarios como es la libertad de información y/o expresión[136]. Para tratar de mitigar este peligro surge la necesidad de transparencia[137] y responsabilidad algorítmica[138]. En este contexto es necesario equilibrar la eficacia de la IA para moderar de manera eficiente contenidos a gran escala —dado el número de usuarios de las grandes plataformas— con la tutela de los derechos fundamentales y la transparencia en su implementación[139].

Desde esta perspectiva, la DSA establece nuevas obligaciones de transparencia y rendición de cuentas para las grandes plataformas —incluidos motores de búsqueda— sobre sus prácticas de moderación y curación de contenidos. En términos generales, a la luz de la DSA y las directrices para la reducción de los riesgos sistémicos en los procesos electorales, las grandes plataformas digitales deben prestar especial atención a la creación de contenidos de IA generativa engañosos, sesgados, falsos o que induzcan a error. A estos efectos, deben contar, en la medida en que sea técnicamente factible, con medidas de reducción del riesgo, como es garantizar que el contenido de IA generativa y otros tipos de medios sintéticos y manipulados sean detectables o garantizar que la información generada por los sistemas de IA se base, en la medida de lo posible, en fuentes fiables en el contexto electoral (como la información oficial de las autoridades electorales pertinentes). Vamos a comenzar con las obligaciones sustantivas y asimétricas que la DSA impone en este ámbito, en particular, a las grandes plataformas digitales, como principales canales de publicación y difusión de contenidos.

1.1. La desinformación como riesgo sistémico para grandes plataformas y motores de búsqueda

38. Dentro de la DSA, la sección 5 del Capítulo III (denominado "Obligaciones de diligencia debida para crear un entorno en línea transparente

136. *Vid.* J. BARATA MIR, "Libertad de expresión y moderación privada de contenidos", *Teorder*, 2022, núm. 32, pp. 88-107; LLANSÓ, E.J., "No Amount of 'AI' In Content Moderation Will Solve Filtering's Prior Restraint Problem", *Big Data & Society,* Abril 2020, (https://journals.sagepub.com/doi/full/10.1177/2053951720920686).

137. Mediante la obligada colaboración con las autoridades, en especial coordinador de servicios digitales y la Comisión europea, dando acceso o informes relativos a datos específicos, incluidos los datos relacionados con algoritmos (Considerando 96).

138. K. CREEL y D. HELLMAN, "The Algorithmic Leviathan: Arbitrariness, Fairness, and Opportunity in Algorithmic Decision-Making Systems", *Canadian Journal of Philosophy*, 2022, vol. 52, pp. 26-43.

139. Principal reflexión final a la que llega, J.J. CASTELLÓ PASTOR "Inteligencia artificial aplicada por las plataformas en línea…", *loc. cit.*

y seguro"), recoge las obligaciones adicionales de gestión de riesgos sistémicos para prestadores de plataformas en línea y de motores de búsqueda en línea de muy gran tamaño. La DSA establece particulares requisitos de diligencia a los prestadores de servicios intermediarios en lo que respecta al modo en que deben hacer frente a los contenidos ilícitos, la desinformación y otros riesgos para la sociedad[140]. El objetivo es garantizar un entorno en línea seguro, predecible y digno de confianza, abordando la difusión de contenidos ilícitos en línea y los riesgos para la sociedad que puede generar la difusión de desinformación u otros contenidos[141]. Concretamente, es el art. 34 (Evaluación de riesgos) el que establece la obligación de detectar, analizar y evaluar con diligencia cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios. En consecuencia, esta evaluación de riesgos será específica de sus servicios (típicamente de intermediación) y proporcionada a los riesgos sistémicos, teniendo en cuenta su gravedad y probabilidad, e incluirá los siguientes riesgos sistémicos: a) la difusión de contenido ilícito a través de sus servicios; b) cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales, en particular los relativos a la dignidad humana amparada por el artículo 1 de la Carta, al respeto de la vida privada y familiar amparada por el artículo 7 de la Carta, a la protección de los datos de carácter personal amparada por el artículo 8 de la Carta, a la libertad de expresión e información, incluida la libertad y el pluralismo de los medios de comunicación, amparada por el artículo 11 de la Carta, a la no discriminación amparada por el artículo 21 de la Carta, a los derechos del niño amparados por el artículo 24 de la Carta y a un nivel elevado de protección de los consumidores, amparado por el artículo 38 de la Carta; c) cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública; d) cualquier efecto negativo real o previsible en relación con la violencia de género, la protección de la salud pública y los menores y las consecuencias negativas graves para el bienestar físico y mental de la persona.

Así pues, todas las grandes plataformas están obligadas a "identificar, analizar y evaluar" los riesgos sistémicos significativos derivados del funcionamiento y la utilización de sus servicios en la Unión y a mitigar estos riesgos (Cdo 84 y art. 34 DSA). Entre esos riesgos se incluye la publicación

140. *Vid*. Considerando 2.

141. Dentro de este entorno en línea seguro que se pretende con este Reglamento, se protegen eficazmente los derechos fundamentales reconocidos en la CDFUE y se facilita la innovación. *Vid*. Considerando 9.

de contenidos ilegales en línea, la difusión de noticias falsas y la protección de los derechos fundamentales (Cdo 51 DSA). Una vez identificados los riesgos, las plataformas deben implantar "medidas de mitigación razonables, proporcionadas y eficaces adaptadas a los riesgos específicos" (Cdo 89, art. 35). De estas disposiciones se extrae que la desinformación es un riesgo sistémico que las grandes plataformas digitales y los motores de búsqueda deben afrontar. Esta labor se aproxima generalmente a través de la moderación y la curación de contenidos.

39. Como ya se ha adelantado, cada vez es más habitual el empleo de la IA para la realización de estas labores de moderación y curación de contenidos en internet por las grandes plataformas digitales y motores de búsqueda. Estos complejos sistemas algorítmicos realizan funciones fundamentales para detectar, restringir y eliminar rápidamente contenidos ilícitos (o incompatibles con las reglas internas o condiciones generales para la prestación de los servicios), en la labor de moderación (proactiva) de contenidos. Asimismo, permiten clasificar información y personalizar resultados en función del comportamiento del usuario (dentro de esa función de curación o recomendación de contenidos). Este creciente uso de la IA por estos agentes digitales se debe al volumen de datos y la velocidad con la que se crea la información y comparte contenido en línea. Ahora bien, su utilización requiere cautela ya que puede conducir a resultados equívocos (propios de los sistemas IA) con el consiguiente impacto negativo sobre los derechos y libertades fundamentales de los usuarios. Este es un factor que deben tener en consideración los grandes prestadores de servicios digitales de la intermediación dentro de la UE, en el cumplimiento de su obligación de mitigar y revisar los "contenidos incorrectos o engañosos, incluida la desinformación" por el riesgo sistémico relacionado con sus servicios, de conformidad con la normativa europea. De esta suerte, la obligación de transparencia y rendición de cuentas impuesta por la DSA[142] (en especial, los arts. 15[143], 24, 27[144] y 42) se manifiesta como un factor relevante para esta consecución, ya que deben informar a la Comisión Europea, entre otras cuestiones[145], sobre

142. J. CRUZ ÁNGELES, "Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso", *CDT* (Octubre 2022), Vol. 14, N.º 2, pp. 294-318.

143. En particular en su letra c) en lo que respecta a la realización de la labor de moderación proactiva por las plataformas.

144. Relativo a las obligaciones de transparencia del sistema de recomendación para aquellas plataformas que realicen esa labor de curación de contenidos personalizada para sus usuarios.

145. La información que por estas grandes plataformas y motores de búsqueda se debe aportar son las relativas a sus actividades de moderación de contenidos, las medidas

sus actividades de moderación y las medidas adoptadas para controlar la visibilidad y accesibilidad de la información (curación). Se trata de requisitos de transparencia adicionales específicamente dirigidos a las plataformas y buscadores de muy gran tamaño, en especial para informar exhaustivamente sobre las evaluaciones de riesgos realizadas y las medidas consiguientes adoptadas de conformidad con esta norma europea[146].

40. La DSA establece los elementos y factores en los que se deben centrar las muy grandes plataformas y motores de búsqueda en esa labor de evaluación de riesgos sistémicos[147]. De esta suerte, han de centrarse en los sistemas u otros elementos que puedan contribuir a los riesgos, incluidos todos los sistemas algorítmicos, en particular, de recomendación y de publicidad; prestando atención a las prácticas conexas de recogida y uso de datos. Asimismo, deben evaluar si sus condiciones generales (términos de uso) y su cumplimiento son adecuados, así como sus procesos de moderación de contenidos, las herramientas técnicas y recursos asignados. Cuando la amplificación algorítmica de la información contribuya a los riesgos sistémicos, dichos prestadores deben reflejarlo debidamente en sus evaluaciones de riesgos. Cuando los riesgos estén localizados o existan diferencias lingüísticas, dichos prestadores también deben tenerlo en cuenta en sus evaluaciones. Al evaluar los riesgos sistémicos identificados estos prestadores deben también centrarse en la información que no sea ilícita, pero que contribuya a los referidos riesgos sistémicos (como es el caso de información no real o engañosa que contribuya a la desinformación). En consecuencia, las grandes plataformas digitales deben dedicar especial atención a cómo se utilizan sus servicios para difundir o amplificar contenidos incorrectos, manipulados o engañosos, lo que incluye la desinformación. En todo caso estos prestadores deben evaluar, en particular, cómo contribuyen a tales riesgos el diseño y el funcionamiento de su servicio, así como la manipulación intencionada y, a menudo, coordinada y el uso de sus servicios, o la infracción sistémica de sus términos generales de servicio. Específicamente la DSA prevé que estos riesgos pueden derivarse del uso no auténtico de los servicios: como es la creación de cuentas falsas, el uso de *bots* o el uso engañoso de un servicio,

---

adoptadas sobre la disponibilidad, visibilidad y accesibilidad de la información facilitada por el destinatario del servicio, así como de cualquier otra restricción o suspensión de contenidos o de cuentas de los usuarios, entre otros datos. Esta información fue remitida a la Comisión Europea el último cuatrimestre de 2023. *Vid.* J.J. CASTELLÓ PASTOR, "Inteligencia artificial aplicada por las plataformas en línea…", *loc. cit.*

146. *Vid.* Considerandos 49, 66 y 100, para completar las disposiciones relativas a estas obligaciones contenidas en los arts. 15 y 27 DSA.

147. *Vid.* Considerando 84.

u otros comportamientos total o parcialmente automatizados, que puedan dar lugar a la difusión rápida y extensa de información al público que sea un contenido ilícito o incompatible con las condiciones generales de una plataforma en línea o un motor de búsqueda y que contribuya a campañas de desinformación.

1.2. Moderación (proactiva) contra contenidos no deseados: en particular los mecanismos automatizados

41. Es indudable que las plataformas en línea (en especial las muy grandes) juegan un papel esencial en la lucha contra la desinformación como riesgo sistémico, en relación con aquellos contenidos que se publican o difunden a través de sus servicios digitales por sus usuarios. La moderación proactiva de contenidos[148] se configura en este sentido como una herramienta esencial para combatir contenidos y cuentas (perfiles) que conculcan las normas o políticas internas de las plataformas en línea y de los buscadores, y en general, para localizar y eliminar contenidos no deseados (potencialmente lesivos, ilícitos, desinformación y otros riesgos para la sociedad, frente a los que deben luchar de conformidad con el art. 34 DSA). Asimismo, se configura como un mecanismo de gobernanza esencial[149] a través del cual se estructura la dinámica participación de los usuarios en estos espacios digitales, se facilita el acceso a la información en la red, al tiempo que permite prevenir y luchar contra los contenidos y actividades ilícitas (o incompatibles con sus condiciones o términos de uso) así como contra las cuentas infractoras[150].

148. La DSA recoge una definición particular de "moderación de contenidos" en su artículo 3 letra t) como "las actividades, estén o no automatizadas, realizadas por los prestadores de servicios intermediarios, que estén destinadas, en particular, a detectar, identificar y actuar contra contenidos ilícitos o información incompatible con sus condiciones generales, que los destinatarios del servicio hayan proporcionado, por ejemplo la adopción de medidas que afecten a la disponibilidad, visibilidad, y accesibilidad de dicho contenido ilícito o de dicha información, como la relegación, la desmonetización de la información, el bloqueo de esta o su supresión, o que afecten a la capacidad de los destinatarios del servicio de proporcionar dicha información, como la supresión o suspensión de la cuenta de un destinatario del servicio".

149. En este sentido, sobre la virtualidad de los mecanismos de moderación de las plataformas, *vid.* J. GRIMMELMANN, "The virtues of moderation", *Yale Journal of Law & Technology*, vol. 17, n.º 42, 2015, pp. 43-109. En especial, define la moderación de contenidos como "el mecanismo de gobernanza que estructura la participación en una comunidad para facilitar la cooperación y evitar los abusos" (p. 47).

150. Desde esta perspectiva se aproxima la moderación de contenidos por B. GANESH y J. BRIGHT, "Countering extremists on social media: challenges for strategic communication and content moderation", *Policy & Internet*, 2020, vol. 12, núm. 1, pp. 6-19,

A más, como ya se anticipó, las políticas de moderación proactivas de los prestadores de servicios digitales de intermediación se ven fomentadas por la legislación (vinculando su uso al régimen de exención de responsabilidad aplicable[151]) y por las instituciones europeas[152]. En este ámbito, significativa importancia se le da en la DSA a los de códigos de conducta (y protocolos de crisis, y otras medidas de autorregulación como medidas de reducción de riesgos) adoptados con estos fines[153]; para cuya adopción deben cooperar con reguladores y expertos para desarrollar estrategias más efectivas contra la desinformación[154]. Expuestas sus virtudes, lo esencial de este mecanismo para su adecuación al marco normativo es la necesaria transparencia en el ejercicio de esta labor, especialmente si se utilizan sistemas de IA (generalmente mediante herramientas de aprendizaje automático predictivo y de comparación automatizadas sobre listas de contenidos ya creados). La razón es poderosa, pues esta actividad incide directamente en el ejercicio de derechos fundamentales como es la libertad de expresión (incluyendo la infor-

---

donde se define como "el conjunto de prácticas utilizadas por las plataformas en línea para hacer cumplir sus directrices sobre contenidos aceptables" (p. 8).

151. Así, el art. 7 de la DSA, establece la aplicación del régimen de exención de responsabilidad (art. 6 en estos casos) a estos prestadores de servicios digitales de intermediación que realicen "investigaciones por iniciativa propia de forma voluntaria, o adopten medidas con el fin de detectar, identificar y retirar contenidos ilícitos, o bloquear el acceso a estos, o adoptar las medidas necesarias para cumplir los requisitos del Derecho de la Unión y del Derecho nacional en cumplimiento del Derecho de la Unión, incluidos los requisitos establecidos en el presente Reglamento". Esta aproximación puede ponerse en relación con la conocida como cláusula del buen samaritano del Derecho estadounidense (sección 230 de la *Communications Decency Act*). Un análisis de esta disposición y su aplicación jurisprudencial, en J. J. CASTELLÓ PASTOR, "Exoneración de responsabilidad de los prestadores de servicios de la información en la sección 230 de la *Communications Decency A*ct estadounidense", *Revista Aranzadi de derecho y nuevas tecnologías*, 2015, núm. 39, pp. 175-194.

152. Desde la Comisión Europea, en la forma de Códigos de buenas prácticas y directrices (art. 35 apdo. 3). A modo de ejemplo, en 2016 se acordó el Código de conducta para combatir el discurso de odio ilegal en línea para prevenir y contrarrestar la propagación del discurso de odio ilegal en línea, por la Comisión y *Facebook, Microsoft, Twitter* y *YouTub*e (https://ec.europa.eu/newsroom/document.cfm?doc_id=42855); posteriormente se han ido adhiriendo otras tecnológicas como *Instagram, Snapchat* y *Dailymotion* en 2018, Jeuxvideo.com en 2019, *TikTok* en 2020, *LinkedIn* en 2021 y *Rakuten Viber* y *Twitch* en 2022). Asimismo, el año 2018 la Comisión Europea introdujo el "Código de Prácticas sobre Desinformación" (disinfocode.eu/) y en el mismo año publicó la Recomendación (UE) 2018/334, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea (C/2018/1177. DO L 63 de 6.3.2018, p. 50/61).

153. *Vid.* Considerandos 104, 106, 108, arts. 45 a 48 DSA.

154. Incluyendo otros prestadores de servicios en línea, para abordar riesgos comunes. *Vid.* Considerandos 102 y 132.

mación) de los usuarios digitales[155]. Ahora bien, aunque los muy grandes prestadores de servicios en línea de intermediación optan principalmente por los mecanismos algorítmicos (sistemas de IA) para estas operaciones de control de contenidos (moderación), por el gran volumen de datos que han de controlarse, no es un sistema exclusivo, sino que típicamente operan con modelos híbridos[156]. De esta forma, además de los mecanismos automatizados cuentan con equipos humanos encargados de identificar, revisar y aplicar o ejecutar las medidas correspondientes sobre los contenidos diarios subidos a sus espacios digitales[157]. Así las cosas, son distintos los modelos por los que las plataformas en línea y motores de búsqueda pueden optar para realizar esa necesaria labor de control de contenidos[158]. Nos centraremos en aquellas cuestiones que plantean el uso de los sistemas de moderación algorítmica.

42. Partiendo de la idoneidad de estos sistemas para gestionar el ingente volumen de datos y la rapidez a la que se crea y comparte el contenido e información en las grandes plataformas —lo que sin duda coadyuva en el objetivo de conseguir entornos digitales más seguros y confiables—, la cuestión fundamental es determinar si esa capacidad también se prodiga en cuanto al fondo. Los sistemas de moderación algorítmica de contenidos manifiestan una precisión insuficiente en la realización de esa labor, lo que unido a la presencia de sesgos, pueden conducir a resultados erróneos en cuanto a la toma de decisiones con significativas consecuencias negativas —particularmente en el ejercicio de derechos y libertades fundamentales—. La propia DSA parte del presupuesto de la existencia de errores en el uso de los sistemas algorítmicos, al establecer que los intermediarios que utilicen estos medios automatizados para moderar contenidos deben incluir "una

155. En este sentido hay doctrina que se manifiesta que la opacidad constatada en estos sistemas de moderación de contenidos es buscada por los operadores digitales. En esta línea, T. GILLESPIE, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media,* Yale University Press, New Haven, 2018, p. 198.

156. Como es el caso de *Facebook* e *Instagram*, de conformidad con la información facilita por Meta a la Comisión Europea el 27 de octubre de 2023 (disponible en: https://transparency.dsa.ec.europa.eu).

157. De esta suerte, el control y la gestión de los contenidos en la plataforma recae tanto en la tecnología IA como a la intervención humana, o en un enfoque híbrido que combina estos dos métodos. *Vid.* K. KLONICK, "The New Governors: The People, Rules, and Processes Governing Online Speech", *Harvard Law Review*, vol. 131, Issue 6, 2018, pp. 1599-1670, en esp. p. 1635.

158. Un análisis de las ventajas e inconvenientes de cada uno de estos modelos puede verse en J. J. CASTELLÓ PASTOR, "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda…", *ob. cit.*, Apdo. II. 1. y doctrina internacional ahí referida.

descripción cualitativa, una especificación de los fines precisos, los indicadores de la precisión y la posible tasa de error[159] de los medios automatizados empleados para cumplir dichos fines, y las salvaguardias aplicadas" en los informes relacionados con las disposiciones de transparencia informativa (art. 15.1.e)[160]. La principal cuestión que plantea el uso de estos mecanismos automatizados es la dificultad en distinguir entre la licitud e ilicitud del contenido publicado por parte de un sistema algorítmico, ya que esta condición no depende solo del contexto de la publicación sino también de la propia intencionalidad de su autor. Los sistemas de IA no suelen tener en consideración todos los datos de contextualización e intencionalidad necesarios para poder calificar la ilicitud[161]; como es, por ejemplo, el contexto histórico, cultural, social o político, o distinguir el carácter satírico, educativo o meramente informativo de la expresión publicada[162].

Así las cosas, el uso de los sistemas de IA en la moderación de contenidos si bien permite a los prestadores digitales intermediarios detectar y reaccionar rápidamente frente a un número ingente de comportamientos ilícitos y perjudiciales en la red, su idoneidad puede plantear, en cuanto al fondo, significativas cuestiones; ya que su utilización puede llevar a resultados equívocos con respuestas que pueden ser erróneas, sesgadas o incluso discriminatorias[163]. De esta suerte, un falso positivo detectado

159. Resulta positivo que la DSA introduzca la consideración de la tasa de error de los modelos algorítmicos (Cdo 26), pero como se ha manifestado la doctrina internacional, una mera recomendación (vaga) se queda corta y su aplicación debería ir más allá. En este sentido, F. G'SELL, "The Digital Services Act: A General Assessment", en *Content Regulation in the European Union. The Digital Services Act* (ed. A. UNGERN-STERNBERG (ed.), vol. 1, pp. 85-118, en esp. p. 92.

160. A más, en el Considerando 26 (en relación con el citado art. 7) establece la necesidad de actuar de buena fe y con diligencia debida por parte de los prestadores de servicios de intermediación en la realización de esas actividades proactivas de detección de contenidos no deseados: moderación de contenidos, para beneficiarse del régimen de exención de responsabilidad. Estableciendo que la condición de actuar de buena fe y con diligencia "debe implicar actuar de manera objetiva, no discriminatoria y proporcionada, teniendo debidamente en cuenta los derechos e intereses legítimos de todas las partes implicadas, y proporcionar las garantías necesarias contra la retirada injustificada de contenidos lícitos, de conformidad con el objetivo y los requisitos del presente Reglamento".

161. N. ELKIN-KOREN Y P. MAAYAN, "Guarding the guardians: content moderation by online intermediaries and the rule of law", en AA.VV.: *Oxford Handbook of Online Intermediary Liability* (ed. por G. FROSIO), Oxford Academic, 2020, Chapter 34, pp. 669-678.

162. *Cf.* T. GILLESPIE, *Custodians of the Internet…, ob. cit.*, p. 169.

163. *Cf.* E. DOUEK, "Content moderation as systems thinking", *Harvard Law Review*, 2022, vol. 136, pp. 526-607, en esp. p. 548.

conllevaría identificar erróneamente el contenido como ilícito (o contrario a las políticas internas del servicio, que no tiene por qué ser lo mismo[164]), lo que supondría censura, además de limitar sin justificación real la libertad de expresión del usuario —ya que se eliminan contenidos legítimos—. A diferencia de lo que ocurre cuando se trata de un caso de un falso negativo, que permitiría que el contenido permanezca en la red, con impunidad al autor y/o difusor del contenido[165]. A esto se le une el problema de la falta de transparencia de las políticas de detención automatizada de contenidos utilizadas por los grandes operadores digitales de la intermediación (agentes privados) que condicionan no solo el comportamiento de sus usuarios digitales —haciendo cumplir sus condiciones de uso so pena de perder el acceso a sus servicios—, sino que en última instancia determinan qué información y contenidos se difunden y distribuyen en Internet[166]. En esta operación de control (proactivo) de contenidos mediante sistemas automatizados, las medidas de retirada o eliminación de contenidos operan ya sea la información calificada como ilícita o como contraria a las políticas internas (condiciones generales o términos de usos de la plataforma). De esta forma, la necesaria calificación de ilícita de una información para que en principio su censura (retirada) esté justificada[167] puede soslayarse —ilicitud que dependerá del ordenamiento jurídico de referencia, en función de la norma de conflicto aplicable por la autoridad competente—; ya que si la información en cuestión no pasa el filtro marcado por las políticas internas[168], aun no siendo ilícito, será retirado. En definitiva, se deja en manos de actores privados, y los algoritmos que ellos deciden, la información que puede diseminarse por la red, lo que es una cuestión —como se ha visto—

164. Si bien, tendría el mismo resultado: retirada del contenido.

165. Véase, E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN y J. HARAMBAM. J.: "Artificial Intelligence, Content Moderation, and Freedom of Expression", *Working paper of the Transatlantic Working Group on Content Moderation Online and Freedom of Expressio*n, 2020, p. 7 (https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf).

166. En este sentido se ha manifestado cierta dotrina internacional. Así, K. KLONICK, señala que la configuración de estas normas de moderación puede afectar al discurso público, a la información en la red y a los derechos individuales de libertad de expresión. *Cfr.* K. KLONICK, "The New Governors", *ob. cit.*, p. 1630.

167. Y no tutelada por el derecho fundamental a la libertad de expresión, incluida de información.

168. En función de los algoritmos en los que se basen esas herramientas automatizadas de control de contenidos; que serán lo que determinen si se cumplen o no las condiciones generales del servicio y de determinar, por lo tanto, lo que constituye un contenido ilícito a los efectos indicados (con independencia de la ley rectora al fondo y de si son realmente contenidos ilícitos a la luz de ese sistema jurídico). En este sentido, es más adecuado hablar de contenidos inapropiados frente al términoilícitos.

más que significativa[169]. Por todo ello, la supervisión por las autoridades competentes de estos mecanismos resulta esencial.

1.3. Curación (recomendación) de contenidos automatizada: peligros en presencia y oportunidades

43. La personalización de los productos y servicios que se ofrecen a los usuarios digitales por las plataformas en línea, al margen de la evidente finalidad económica de esta funcionalidad (ya que es una parte fundamental de su negocio[170]), también pueden servir para coadyuvar en la lucha contra los contenidos no deseados (dentro del deber de evaluar y mitigar los riesgos sistémicos). Así las cosas, la curación de contenidos cumplirá la función de lucha contra la desinformación (como riesgo sistémico) en la medida que se implementen algoritmos de recomendación para priorizar contenidos confiables y reducir la visibilidad de la desinformación. Sin duda la utilización de la IA en este sentido supone una revolución en la gestión de grandes cantidades de datos y personalización de contenido, pero también implicaciones éticas en cuanto al control y administración del contenido digital que se ofrece a los usuarios. Lo determinante es la adecuación del sistema algorítmico utilizado para realizar esa recomendación personalizada para cumplir con este deseado objetivo. Vamos a ver brevemente cómo funcionan estos sistemas en este ámbito para concretar su virtualidad a los efectos marcados, así como los peligros en presencia, en especial en relación con la desinformación.

44. Para la realización de la función de curación se utilizan generalmente por los prestadores de servicios de plataformas en línea sistemas algorítmicos de recomendación de contenidos que filtran, priorizan y presentan la información que más se ajusta a las preferencias del usuario[171]. En conse-

169. Lo que condiciona la consecución de esa gobernanza digital que se pretende por la UE garantizando todos los derechos y libertades fundamentales en juego, siendo uno de los principales desafíos a afrontar. Para J.J. CASTELLÓ PASTOR, la ausencia de una exhaustiva normativa que regule de la gobernanza de los servicios digitales permite que estos actores privados establezcan sus propias políticas internas de cumplimiento, con las consecuencias indicadas. Para este autor, esto conduce, indirectamente, a que "la regulación de la sociedad digital esté en manos de unos pocos gigantes tecnológicos", que controlan el acceso y la información que es visible en la red, "ganando cada vez más relevancia para el funcionamiento del ecosistema digital". En "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda…", *ob. cit.*, Apdo. II. 1. A) y doctrina internacional ahí referida.

170. Y así lo recoge el considerando 70 DSA.

171. Se trata de la información que le aparece al usuario digital en el interfaz en línea de acuerdo con la información facilitada por el propio usuario en el registro (previo para

cuencia, el funcionamiento de estos sistemas de recomendación[172] influyen significativamente en la capacidad del usuario para recuperar la información e interactuar con ella[173]. Es indudable que estos sistemas algorítmicos de curación de contenidos mejoran significativamente la experiencia digital de cualquier usuario (pudiéndose centrar en aquellos temas con los que tiene mayor interés), pero su utilización no está exenta de potenciales consecuencias negativas. Dejando al margen los riesgos asociados por el diseño adictivo de las interfaces en línea[174], por el objeto de estudio nos centraremos en el peligro real de aislamiento del usuario de otras informaciones y contenidos reales, ya que la personalización de la información puede aislar al usuario (creándose lo que ya se ha referido como "burbuja de filtro[175]"). En estos

---

disponer de acceso) al servicio o, por ejemplo, recogida de los datos de navegación (por el rastreo y seguimiento) de las cookies.

172. En este sentido se define en la DSA el sistema de recomendación como "un sistema total o parcialmente automatizado y utilizado por una plataforma en línea para proponer en su interfaz en línea información específica para los destinatarios del servicio o priorizar dicha información, también como consecuencia de una búsqueda iniciada por el destinatario del servicio, o que determine de otro modo el orden relativo o la relevancia de la información presentada" (art. 3 letra s)

173. Esto resulta especialmente significativo en relación con los motores de búsqueda. En estos casos, la oferta de los bienes y servicios viene en gran medida por la posición de los operadores económicos en el buscador, ya que raramente los usuarios pasan de la segunda página de los resultados ofrecidos. *Vid.* J. GRIMMELMANN, "The structure of search engine Law", *Iowa Law Review*, 2007, vol. 93, n.º 1, pp. 1-63, en esp. p. 31.

174. Cuestión que no es objeto de estudio. Nos limitaremos a indicar que la DSA establece obligaciones especificas al respecto para las plataformas en línea. En especial, véase el art. 25 en relación con el diseño y organización de la interfaz en línea. Sobre el particular, J. CORBERÁ MARTÍNEZ, "Diseño y organización de interfaces en línea en el Reglamento de servicios digitales", en AA.VV.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2024, pp. 171-200. También en relación con la publicidad digital se contienen medidas de obligada observancia en la DSA. Sobre esta cuestión, *vid.* R. LAPIEDRA ALCAMÍ, "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad digital", en la misma obra colectiva (pp. 205-226). De lo relevante de la cuestión, da muestra la Resolución aprobada por el Parlamento Europeo (2023/2043(INI) de 12 de diciembre de 2023 sobre el Diseño adictivo de servicios en línea y protección del consumidor en el mercado único de la UE. En este documento se insta a la Comisión a que valore y supla las lagunas regulatorias existentes en relación con las vulnerabilidades de los consumidores, los patrones oscuros (y de personalización manipuladora) y las características adictivas de los servicios digitales, especialmente aquellos dirigidos a menores.

175. Esto supone que es la plataforma (típicamente redes sociales) la que delimita al usuario qué noticias, contenidos, perfiles lee a través de sus servicios, ofreciendo personalmente, según sus algoritmos, la información que debe consumir (personalización de resultados) Esta práctica puede ser peligrosa y una fuente de desinformación, si los

casos, el "aislamiento" del usuario se ve retroalimentado por el propio algoritmo, que muestra al destinatario únicamente aquella información de corte similar a sus preferencias, permitiéndose así la amplificación de los mensajes, la difusión viral del contenido y la promoción de comportamientos en línea afines al destinatario del servicio; excluyendo, por lo tanto, cualquier dato de otra índole. En este sentido, no solo en el contexto específico de un proceso electoral esta funcionalidad se manifiesta controvertida, ya que en términos generales la selección de contenidos sensibles y de naturaleza extremista —sobre la base de complejos algoritmos predictivos— está conduciendo a una sociedad cada vez más polarizada y dividida[176]. Al margen, además, de aquellos contenidos "recomendados" que puedan ser peligrosos para la salud e integridad del propio usuario[177]. Por ello, el sistema de recomendación de contenidos puede tener un significativo impacto negativo no solo para los usuarios digitales (como individuo o incluso grupo), sino también para la propia sociedad en su conjunto.

La DSA parte de esta realidad y del más que potencial peligro que plantean los sistemas de recomendación (automatizado) de los prestadores digitales de intermediación[178]. Así, cuando se presentan a los usuarios digitales anuncios basados en técnicas de segmentación optimizadas para responder a sus intereses y apelar potencialmente a sus vulnerabilidades, se entiende que los efectos negativos pueden ser especialmente graves. De hecho, se habla textualmente de "técnicas de manipulación" que pueden afectar negativamente a grupos enteros y amplificar perjuicios sociales; por ejemplo, contribuyendo a campañas de desinformación o discriminando a determinados grupos. De esta suerte, las plataformas en línea son entornos

---

contenidos con los que únicamente se "bombardea" al usuario son sesgados, propagandísticos, etc., especialmente en el marco de unas elecciones democráticas. En todo caso, se manifiesta el peligro sobre la libertad de pensamiento del individuo (ya que impide la pluralidad de información o acceso a ésta). En este sentido, sobre este fenómeno, con un análisis de los algoritmos E. PARISER, *The filter bubble: What the internet is hiding from you*, New York: Penguin Press, 2011.

176. *Vid*. J. J. CASTELLÓ PASTOR, "Inteligencia artificial aplicada por las plataformas en línea…", *ob. cit.*, Ado. II.2.

177. A modo de ejemplo, Amnistía Internacional en 2023 público un informe titulado "Empujados a la oscuridad: feed 'para ti' de TikTok promueve la autolesión y el pensamiento suicida" (POL 40/7350/2023). Según este estudio, esta red social mediante una "hiperpersonalización" ha creado una plataforma adictiva, y el sistema algorítmico analizado expone a menores de 13 años a vídeos que podrían verse fácilmente arrastrados hacia contenido potencialmente dañino, incluyendo material que idealiza y promueve la depresión, autolesiones y suicidio (https://www.amnesty.org/es/documents/pol40/7350/2023/es/)

178. *Vid.* Considerando 69.

especialmente delicados para tales prácticas y plantean un riesgo mayor para la sociedad; lo que justifica la imposición de obligaciones y prohibiciones adicionales, especialmente para los prestadores de servicios con la consideración de muy gran tamaño. El punto de partida son las obligaciones y requisitos establecidos en el art. 27, vinculados a la transparencia de los sistemas de recomendación utilizados para informar a los usuarios. En síntesis, los operadores que los empleen deben de indicar en las condiciones generales información, de forma clara y comprensible, los parámetros principales utilizados en estos sistemas y sobre cualquier opción que tenga el destinatario del servicio para adaptarlos[179]. Se completa la materia con requisitos y prohibiciones vinculadas a la privacidad y protección de datos personales de los usuarios[180]. Entre estas últimas destaca la obligación de los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño que utilicen sistemas de recomendación, de ofrecer al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles tal como se define en el artículo 4, punto 4, del RGPD[181]. Asimismo, y en particular, se articulan específicas obligaciones de diligencia debida para estos operadores de muy gran tamaño en este contexto. Estas obligaciones se extienden a las medidas adoptadas por las plataformas para probar y, en su caso, adaptar sus sistemas algorítmicos; en especial, sus sistemas de recomendación[182]. De esta suerte, pueden tener que mitigar los efectos negativos de las recomendaciones personalizadas y corregir los criterios utilizados en sus recomendaciones, si se aprecia por las autoridades que es necesario.

179. Véase. artículo 27 *in fine* DSA.
180. En consecuencia, se establece la prohibición a los prestadores de plataformas en línea de presentar anuncios basados en la elaboración de perfiles (en los términos del art. 4, punto 4, RGPD), utilizando las categorías especiales de datos personales a que se refiere el art. 9, apartado 1, de dicho Reglamento, ni utilizando categorías de elaboración de perfiles basadas en dichas categorías especiales. Esta prohibición complementa el resto de obligaciones que, en materia de protección de datos personales, les corresponda cumplir a estos agentes o a cualquier otro prestador de servicios o anunciante que participen en la difusión de los anuncios en virtud del Derecho de la Unión (Cdo. 69).
181. Así se manifiesta el Considerando 94, en relación con datos personales y elaboración de perfiles. Además, y como complemento de las obligaciones de transparencia aplicables a las plataformas en línea en lo que respecta a sus sistemas de recomendación (art. 27), las plataformas y buscadores de muy gran tamaño deben garantizar sistemáticamente que los destinatarios de su servicio disfruten de opciones alternativas que no se basen en la elaboración de perfiles, en el sentido del RGPD, para los parámetros principales de sus sistemas de recomendación. Estas opciones deben ser directamente accesibles desde la interfaz en línea en la que se presentan las recomendaciones.
182. *Vid*. Cdo. 88.

45. En todo caso, más allá de los evidentes peligros que la función de curación o recomendación puede conllevar a los usuarios (individuos, grupos) e incluso a la sociedad en su conjunto, según el sistema algorítmico utilizado, el legislador europeo reconoce que los sistemas publicitarios (de recomendación) utilizados por las plataformas y motores de búsqueda en línea de muy gran tamaño pueden ser un catalizador de riesgos sistémicos. Así las cosas, estos prestadores mediante medidas correctoras (como suspender la recaudación de ingresos por publicidad de información específica, u otro tipo de medidas) pueden analizar cómo mejorar la visibilidad de fuentes autorizadas de información, o de forma más estructural adaptar sus sistemas de recomendación. A estos efectos, las muy grandes plataformas y motores de búsqueda pueden tener que reforzar sus procesos internos o la supervisión de cualesquiera de sus actividades, en particular en lo que respecta a la detección de riesgos sistémicos, y realizar evaluaciones de riesgos más frecuentes o específicas relacionadas con esta función de recomendación. Concretamente, en la medida que se trate de riesgos compartidos, las plataformas en línea deben colaborar con otros prestadores de servicios, por ejemplo mediante la adopción de nuevos códigos de conducta (o de buenas prácticas) o la suscripción a los ya existentes, u otras medidas de autorregulación —en los mismos términos a los ya expuestos en relación con el control de contenidos o moderación proactiva para eliminar información no deseada—[183]. A mayor abundamiento, cuando los riesgos estén relacionados con campañas de desinformación incluso estos operadores digitales deben sopesar medidas de concienciación[184].

2. LA COMISIÓN EUROPEA EN LA LUCHA CONTRA LA DESINFORMACIÓN EN LAS REDES

46. Antes de entrar a abordar las concretas acciones e iniciativas de las autoridades europeas (en particular la Comisión) para la lucha contra la desinformación a través de los servicios de los prestadores de plataformas digitales de intermediación y motores de búsqueda, vamos a referir algunos de los más significativos supuestos de investigación que se encuentran en curso dentro de la UE. Se trata de procedimientos instados en relación con actividades de determinadas muy grandes plataformas en línea en las que ha intervenido la IA (en particular sistemas algorítmicos de recomendación

183. En particular en el ámbito de la lucha contra la desinformación se constatan iniciativas de la Comisión europea suscritas por un número significativo de redes sociales. *Vid. infra* Apdo. III.2.

184. *Vid.* Cdo. 88 y art. 35 letra i).

así como medidas de moderación de contenidos) y su compatibilidad con las disposiciones impuestas por la DSA para este campo. Concretamente nos centraremos en los procedimientos formales incoados por la Comisión Europea: primero frente a la red social *TikTok* en relación con contenidos electorales relativos a las elecciones nacionales de Rumania; en segundo lugar, frente a la plataforma *X* (anterior *Twitter*) por las constantes reclamaciones de injerencia en los procedimientos electorales en distintos países de la UE por los contenidos difundidos por esta red, manifestados por distintas autoridades nacionales desde el año 2023. Para finalizar abordaremos la situación del grupo Meta (respecto de sus principales redes sociales: *Facebook* e *Instagram*) y las eventuales consecuencias de los últimos movimientos de este grupo en relación con sus sistema de verificación a la luz de la normativa europea.

2.1. Investigaciones en curso frente a muy grandes plataformas para mitigar riesgos en procesos electorales y discursos cívicos: los casos de TikTok, X y Meta

47. El punto de partida son las obligaciones sustantivas que la DSA impone a las declaradas como plataformas en línea de muy gran tamaño (redes sociales), transcurridos cuatro meses tras su designación como tales, que les son exigibles en este ámbito concreto[185]; pues la verificación de su cumplimiento —y sus consecuencias— es el objeto general de los procedimientos formales de investigación incoados por la Comisión a los que nos referiremos[186].

48. En el marco del desarrollo de las elecciones nacionales rumanas (celebradas entre el 24 de noviembre de 2024 y el 31 de marzo de 2025), a finales de noviembre de 2024 la Comisión solicitó información a la red social *TikTok*[187] para determinar qué medidas había tomado la plataforma para reducir el posible sesgo algorítmico en ese proceso electoral (lo que ya de por sí suponía la primera fase de una posible investigación formal que luego como tal se materializó). Como resultado de la primera vuelta de las elecciones presidenciales en este Estado miembro (desarrolladas el 24 de noviembre de 2024), obtuvo la victoria *Calin Georgescu*, un candidato

185. *Vid. supra* Apdo. III.1.

186. *Vid.* Cap. IV, secc. 4 (Supervisión, investigación, ejecución y seguimiento respecto de los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño).

187. Declarada el 25 de abril de 2023 por la Comisión como plataforma de muy gran tamaño a los efectos de la DSA, junto con otras 16 muy grandes plataformas y 2 muy grandes motores de búsqueda. De conformidad con la información publicada por la UE https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

nacionalista independiente y euroescéptico poco conocido hasta entonces por el público. A mayor abundamiento, concurre las circunstancias de que estas elecciones fueron anuladas después de que el Tribunal Constitucional[188] de este país recibiera pruebas de la injerencia rusa en el proceso de votación, en particular a través de la red *TikTok*, según información facilitada por los servicios de inteligencia rumanos[189]. Esto conlleva repetir las elecciones en dicho país[190]. En este contexto, el 5 de diciembre de 2024, la Comisión europea emitió una orden de retención[191], ordenando a esta plataforma que congelara y conservara los datos relacionados con los riesgos sistémicos reales o previsibles que su servicio podría plantear en los procesos electorales y el discurso cívico en la UE; lo que suponía la entrega de datos sobre sus sistemas de recomendación desde el 24 de noviembre hasta el 21 de marzo de 2025 para su posterior análisis. El 6 de diciembre de 2024, tras la desclasificación de documentos de los servicios de inteligencia rumanos sobre injerencias en el procedimiento electoral a través de campañas llevadas a cabo en la plataforma *TikTok*, la Comisión emitió una solicitud de información urgente exigiendo a la red más respuestas sobre su papel en la primera vuelta de las elecciones presidenciales de Rumanía, dadas las presunciones de injerencia extranjera[192]. Así las cosas, el 17 de diciembre 2024 la Comisión abrió un procedimiento formal[193] para investigar a esta

188. Fuente *euronews.com*: C. CARABALLO, "Anulan las elecciones presidenciales en Rumanía tras las denuncias de interferencia extranjera", 08/12/2024, https://es.euronews.com/my-europe/2024/12/08/anulan-las-elecciones-presidenciales-en-rumania-tras-las-denuncias-de-interferencia-extran (última consulta 7 de enero 2025). También esta información en https://es.euronews.com/my-europe/2024/12/06/el-tribunal-constitucional-rumano-bloquea-la-segunda-vuelta-de-las-presidenciales; https://edition.cnn.com/2024/12/06/europe/romania-annuls-presidential-election-intl/index.html

189. Mediante informes de inteligencia desclasificados por las autoridades rumanas, así como los informes de terceros. os servicios de inteligencia rumanos que mostraban la implicación de Rusia para influir en los votantes mediante una campaña de propaganda antioccidental en apoyo de *Georgescu*. La investigación llevada a cabo por la Comisión también sigue el análisis de los informes de evaluación de riesgos presentados por esta red social en 2023 y 2024, las respuestas a las solicitudes de información de la Comisión y los documentos internos facilitados por *TikTok* (https://transparency.dsa.ec.europa.eu).

190. Posteriormente, en fecha de 9 de marzo de 2025 la Oficina Electoral Central (BEC) rumana rechazó la candidatura de *Călin Georgescu* a las elecciones presidenciales. Esta resolución, susceptible de recurso frente al Tribunal constitucional, fue ratificada por el Constitucional dos días después (11 de marzo).

191. Toda la información sobre esta orden de retención en https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243

192. https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487

193. Coimisiún na Meán, el coordinador de servicios digitales de Irlanda (país de establecimiento de la red en la UE) participa en la investigación de la Comisión Europea.

red social[194] ante posibles injerencias en estas elecciones, por la información difundida a través de esta plataforma[195]. Dentro del marco de este procedimiento formal se está tratando de recopilar todos datos para determinar si esta plataforma infringió las obligaciones recogidas en la DSA vinculadas al control y mitigación de riesgos sistémicos[196] —en los términos anteriormente expuestos—, al no mitigar adecuadamente los riesgos relacionados con la integridad de las elecciones en Rumanía.

Entre otras cuestiones, es la labor de curación realizada por esta plataforma, a través de su sistema algorítmico (IA), lo que está bajo investigación y se vincula con nuestro objeto de estudio. Las actuaciones de la plataforma en las que se centra la investigación, en lo que respecta a la gestión de los riesgos para las elecciones o el discurso cívico, están vinculadas a los sistemas de recomendación de la red[197], en particular los riesgos relacionados con la manipulación no auténtica coordinada o la explotación automatizada del

194. No es el primer procedimiento formal incoado por la comisión contra esta red social. Esta es la tercera investigación que la Comisión ha iniciado contra TikTok, tras la investigación en curso abierta el 19 de febrero de 2024 (https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926) y la investigación iniciada en abril y cerrada con compromisos en agosto de 2024 (https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227). La primera de ellas, aún pendiente, se fundamenta en posibles incumplimientos de la DSA de esta plataforma en relación con la protección de los menores, la transparencia publicitaria, el acceso a los datos para los investigadores, así como la gestión de riesgos del diseño adictivo y los contenidos nocivos. Respecto de la investigación abierta en abril, fue posteriormente cerrada en agosto de 2024, pues se resolvió de *facto*, ya que *TikTok* ha retirado el despliegue de *TikTok Lite* (que habría recompensado a los usuarios por el tiempo dedicado a determinadas "tareas" en la red, como ver vídeos, recibir contenidos, seguir a los creadores, invitar a amigos a unirse a *TikTok*....), después de que la Comisión manifestara sus preocupaciones sobre el impacto potencial de la aplicación en la salud mental y los riesgos de adicción entraban en conflicto con la DSA (al no cumplir con la preceptiva evaluación previa y diligente de los riesgos que conlleva, en particular los relacionados con el efecto adictivo de las plataformas, y sin adoptar medidas eficaces de reducción de riesgos).

195. *Vid.* R. ARMANGAU, "La Comisión Europea ha incoado un procedimiento formal contra TikTok por posibles infracciones de la Ley de Servicios Digitales, a raíz de las pruebas de injerencia rusa en las elecciones de Rumanía. Bruselas está recopilando datos para determinar si TikTok infringió la legislación de la UE", Publicado 17/12/2024. https://es.euronews.com/my-europe/2024/12/17/la-comision-europea-abre-una-investigacion-contra-tiktok-por-las-elecciones-en-rumania Todos los datos de este procedimiento, los antecedentes y las siguientes fases en https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487

196. Artículos 34, apartados 1 y 2, y 35, apartado 1.

197. Respecto de los sistemas algorítmicos utilizados por la plataforma se plantean si los contenidos concretos en favor del referido candidato son consecuencia del sistema y los algoritmos de *TikTok* o si se modificó deliberadamente sus algoritmos para que

servicio; así como a su políticas sobre publicidad política y contenido político de pago[198]. En ambos casos la DSA impone, entre otras, unas específicas obligaciones de transparencia y etiquetado claro. Estamos ante una primea fase del procedimiento formal en la que se trata de recabar por la Comisión toda la información necesaria para determinar si *TikTok* ha infringido la DSA en las concretas obligaciones de diligencia implicadas[199] (en especial, si la red ha mitigado diligentemente los riesgos que plantean los aspectos regionales y lingüísticos específicos de las elecciones nacionales). La investigación que hasta el momento se ha realizado ha permitido constatar que los contenidos publicitarios sobre el referido candidato (*Georgescu*) proliferaron en esta plataforma justo antes de la primera votación. La Comisión valora si estos contenidos pudieran haber sido promovidos por *bots* y cuentas falsas[200].

Tras la incoación formal, la Comisión seguirá reuniendo pruebas para poder tomar una decisión (por ejemplo, enviando solicitudes adicionales de información, llevando a cabo acciones de seguimiento, entrevistas, inspecciones y solicitando acceso a algoritmos utilizados por la plataforma para el desarrollo de sus actividades y prestación de sus servicios en línea). Estas solicitudes de información podrán exigir a la plataforma que facilite datos y documentos que tendría la obligación de conservar sobre la base de la referida orden de conservación (retención) impuesta el 5 de diciembre de 2024. Asimismo, la incoación de procedimiento formal faculta a la Comisión a adoptar nuevas medidas de ejecución, como medidas provisionales y decisiones de incumplimiento en relación con este operador digital. En cualquier caso, la Comisión podrá aceptar cualquier compromiso asumido por la red *TikTok* (si es que los hay)[201] para remediar los asuntos objeto del procedimiento para su conclusión. Solo se exponen los posibles escenarios, pues habrá que esperar el resultado de este procedimiento y su conclusión

---

cada vez más usuarios rumanos recibieran y creyeran que toda Rumanía quiere a un determinado candidato, condicionando su decisión en el procedimiento electoral.

198. Según el Servicio de Inteligencia Rumano (SRI), casi un millón de euros fueron gastados en la campaña por una persona que apoyaba la candidatura de *Georgescu*, con hasta 950 euros pagados por un reenvío. La propia plataforma admitió haber recibido 362.500 euros de esta persona la semana pasada, según mostraron los documentos. Los datos concretos han sido extraídos de https://es.euronews.com/my-europe/2024/12/06/la-ue-exige-respuestas-urgentes-a-tiktok-sobre-la-posible-injerencia-extranjera-en-las-ele

199. Artículo 34, apartados 1 y 2, y del artículo 35, apartado 1, DSA.

200. En relación con su campaña de influencia masiva a favor del candidato presidencial prorruso y anti-UE. Fuente: https://es.euronews.com/2024/11/27/el-candidato-rumano-mesias-de-tiktok-es-un-estreno-crudo-para-europa

201. De conformidad con el art. 71 DSA.

(todavía no se conoce el calendario en el que la Comisión manifieste sus conclusiones[202]). Todo ello sin perjuicio de cualquier otro procedimiento que la Comisión decida incoar en virtud de otras disposiciones de la DSA frente a este mismo agente[203]. Si finalmente se determina que incumple con la legislación, de conformidad con las sanciones previstas en este instrumento, la red social podría enfrentarse a una multa de hasta el 6% de sus ingresos globales (lo que no es una cuestión baladí).

49. Otra muy gran plataforma digital[204] que opera en Europa y que está actualmente bajo investigación formal (desde diciembre de 2023[205]) por parte de la Comisión es la red *X* (anteriormente *Twitter*), por sospecha de falta de neutralidad en cuanto a la información que se divulga a través de esta plataforma, con acusaciones de manipulación. De hecho, son constantes las denuncias por distintas autoridades nacionales de países de la UE que manifiestan injerencias de esta plataforma en diferentes procesos electorales, en ámbitos relacionados con la difusión de contenidos ilícitos y la eficacia de las medidas adoptadas por la red para combatir la manipulación de la información. Para el análisis del posible incumplimiento, como prestador de servicios intermediario, de su obligación de actuar con neutralidad y sin injerencias (especialmente en el contexto de procesos electorales y discurso cívico) es necesario diferenciar entre dos supuestos. Por un lado, la información que el propietario de la plataforma (*Elon Musk*) puede publicar

202. La DSA no establece ningún plazo legal para poner fin a un procedimiento formal como el referido. La duración de la investigación depende de varios factores, entre ellos la complejidad del asunto, la medida en que la empresa en cuestión coopera con la Comisión y el ejercicio del derecho de defensa. Habrá que esperar para saber los resultados de este procedimiento y las consecuencias (económicas) que en caso de verificarse la infracción de las disposiciones de la DSA conlleve a esta plataforma; lo que previsiblemente salga posteriormente a la publicación/revisión de este trabajo.

203. Las medidas de investigación y sanción que pueden adoptar las autoridades nacionales y la Comisión en el ámbito de la DSA, en particular, el desarrollo del procedimiento de ejecución, las medidas que se pueden instar, las competencias de ejecución de la Comisión: de investigación y sancionadoras, pueden consultarse en https://digital-strategy.ec.europa.eu/es/policies/dsa-enforcement

204. La red *X*, anteriormente conocida como *Twitter*, fue designada plataforma en línea de muy gran tamaño el 25 de abril de 2023 en virtud de la DSA, tras su declaración de llegar a más de 45 millones de usuarios activos mensuales en la UE. *Vid*. nota 187.

205. Mediante comunicado de prensa de fecha 18 de diciembre de 2023 se comunicó que La Comisión inició un procedimiento formal contra X en virtud de la DSA. Información disponible en https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6709 Este es primer procedimiento formal iniciado por la Comisión para hacer cumplir el primer marco horizontal a escala de la UE en materia de responsabilidad de las plataformas en línea establecido por la DSA desde su entrada en aplicación.

en su perfil queda fuera del objeto de estudio —y de ella respondería personalmente, en su caso, como responsable de los contenidos publicados y difundidos en su perfil, si estos contenidos no estuvieran tutelados por la libertad de expresión—. Distinto es el caso de la potencial responsabilidad de la propia plataforma, y exigencia del cumplimiento de las obligaciones impuestas por la DSA, respecto de la información que se potencia (se recomienda) por la red (a través de sus algoritmos), así como aquella que no se verifica (moderación), que permitan la difusión de contenidos ilícitos y no deseados, ya sea de usuarios reales o de cuentas falsas o *bots*. Es en este último caso en el que se pueden y deben centrar los procedimientos de investigación institucional de la UE, esto es, ante posibles incumplimientos de las obligaciones impuestas por la DSA a esta red al desarrollar sus servicios dentro de la UE. En este contexto, la Comisión a finales de 2023 inició un procedimiento formal[206] para evaluar específicamente si *X* pudiera haber infringido la DSA en ámbitos relacionados con la gestión de riesgos, la moderación de contenidos, las interfaces engañosas, la transparencia de la publicidad y el acceso de los investigadores a los datos. La apertura de este procedimiento formal se justificaba sobre la base de la investigación preliminar realizada hasta esa fecha, concretamente del análisis del informe de evaluación de riesgos presentado por *X* en septiembre 2023, del informe de transparencia publicado el 3 de noviembre de ese mismo año[207] y de las respuestas de este proveedor de plataforma en línea a una solicitud formal de información dirigida por la Comisión[208]. El procedimiento formal de infracción contra *X* se centra en varias cuestiones. En primer lugar, el cumplimiento de las obligaciones relacionadas con la lucha contra la difusión de contenidos ilícitos en la UE. En particular, en relación con la evaluación de riesgos y las medidas de mitigación adoptadas por *X* para contrarrestar la difusión de contenidos ilícitos, así como el funcionamiento del mecanismo de notificación y acción en relación con los contenidos ilícitos y los recursos de moderación de contenidos de *X*. Por otro lado, se analiza la eficacia de las medidas adoptadas por la red para luchar contra la manipulación de la información en la plataforma; sobre todo la eficacia

206. Toda la información de este procedimiento formal incoado el 18 de diciembre de 2023 en la página https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6709

207. Informe sobre las actividades de moderación de contenido de la plataforma *X, Twitter International Unlimited Company* (TIUC), bajo la Ley de Servicios Digitales (DSA), durante el rango de fechas del 1 de abril de 2024 al 30 de septiembre de 2024. Informe completo disponible en https://transparency.x.com/dsa-transparency-report.html

208. Que, entre otras cosas, se refería a la difusión de contenidos ilícitos en el contexto de los ataques terroristas de Hamás contra Israel. Toda la información sobre esta solicitud en https://ec.europa.eu/commission/presscorner/detail/es/ip_23_4953

del denominado sistema de notas comunitarias de *X* en la UE y la eficacia de las políticas conexas para mitigar los riesgos desde el punto de vista del discurso cívico y los procesos electorales. También las medidas adoptadas por *X* para aumentar la transparencia de su plataforma son objeto de investigación. La investigación se refiere a presuntas deficiencias a la hora de conceder a los investigadores acceso a los datos de acceso público de X, de conformidad con lo dispuesto en el art. 40 DSA, así como a deficiencias en su repositorio de anuncios. Por último, se investiga un presunto diseño engañoso de la interfaz de usuario, sobre todo en relación con las marcas de verificación vinculadas a determinados productos de suscripción, las llamadas marcas azules[209].

Por el momento la Comisión sólo ha presentado unas conclusiones preliminares[210] a *X* por incumplimiento de la DSA (14 de julio de 2024)[211]. Estas conclusiones se manifiestan en relación con tres reclamaciones. En primer lugar, se concluye que X diseña y explota su interfaz para las "cuentas verificadas" con la "marca de control azul" de una manera que no se corresponde con la práctica del sector y engaña a los usuarios. Toda vez que cualquier persona puede suscribirse para obtener este estado "verificado", esto afecta negativamente a la capacidad de los usuarios para tomar decisiones libres e informadas sobre la autenticidad de las cuentas y el contenido con el que interactúan. Se afirma que existen pruebas de que hay agentes malintencionados motivados que abusan de la "cuenta verificada" para engañar a los usuarios. En segundo lugar, se concluye que la red X no respeta la transparencia requerida en materia de publicidad, ya que no proporciona un repositorio de anuncios publicitarios fiable y accesible, sino que establece características de diseño y barreras de acceso que hacen que el repositorio no sea apto para su finalidad de transparencia con respecto a los usuarios. En particular, el diseño no permite la supervisión y la investigación necesarias de los riesgos emergentes derivados de la distribución de publicidad en línea. En tercer y último lugar, para la Comisión la plataforma X no proporciona acceso a sus datos públicos a los investigadores que se adecuen a las condiciones establecidas en la normativa. En particular, la red prohíbe a los investigadores elegibles acceder de forma independiente a sus datos

209. Si se confirmara todas estas deficiencias supondría el incumplimiento por esta red del art. 34, apdos. 1 y 2, art. 35, apdo. 1, art. 16, apdos. 5 y 6, art. 25, apdo. 1, art. 39 y art. 40, apdo. 12, de la DSA.

210. De conformidad con el art. 73 apdo. 2 DSA.

211. Sobre la base de la investigación realizada que incluyó, entre otros datos, el análisis de los documentos internos de la empresa, entrevistas con expertos, así como la cooperación con los coordinadores nacionales de servicios digitales.

públicos, por ejemplo raspando[212], como se indica en sus condiciones de servicio. A mayor abundamiento, para la Comisión el proceso establecido por la red *X* para conceder a los investigadores elegibles acceso a su interfaz de programación de aplicaciones (API), parece disuadir a los investigadores de llevar a cabo sus proyectos de investigación o no les deja más opción que pagar tasas desproporcionadamente elevadas.

Estas son conclusiones preliminares, que se establecen sin perjuicio del resultado de la investigación; ya que la red social *X* tiene ahora la posibilidad de ejercer su derecho de defensa examinando los documentos del expediente de investigación y respondiendo por escrito a las conclusiones. Paralelamente, se consultará a la Junta Europea de Servicios Digitales[213]. Si finalmente se confirmaran los puntos de vista preliminares de la Comisión, ésta adoptaría una decisión de incumplimiento[214] en la que declararía que *X* infringe los artículos 25, 39 y 40 (apdo. 12) de la DSA. Como en el caso anterior analizado, esta decisión podría implicar multas de hasta el 6 % del volumen de negocios total anual mundial del prestador y ordenar al proveedor que adopte medidas para hacer frente a la infracción[215]. Una decisión de incumplimiento también podría dar lugar a un período de supervisión reforzado para garantizar el cumplimiento de las medidas que el prestadores de plataformas en línea se propone adoptar para subsanar la infracción[216]. Asimismo, la Comisión también puede imponer multas coercitivas para obligar a una plataforma a cumplir[217].

50. En último lugar, vamos a referir la investigación abierta por la Comisión sobre *Meta*, en el marco del DSA, en relación con la forma en que *Instagram* y *Facebook*[218] abordaron la desinformación durante la campaña de las elecciones europeas[219]. Las presuntas infracciones que se investigan por la

212. El raspado de datos consiste en extraer datos de sitios web de redes sociales como *X, Instagram, Facebook* y sitios web de *blogs*. El raspado requiere un *software*, conocido como raspador web, que extrae datos automáticamente de los canales de redes sociales.
213. De acuerdo con el art. 61 apdo. 2 letra c) *DSA.*
214. De conformidad con el art. 73 apdo. 5 DSA.
215. Art. 74, apdo. 1 DSA.
216. Así lo prevé el art. 75 DSA, especialmente cuando se trata del incumplimiento de disposiciones del capítulo III, sección 5, como son las obligaciones de evaluación, control y mitigación de riesgos sistémicos, como es la desinformación.
217. Previstas en el art. 76. El cumplimiento de las obligaciones pertinentes impuestas en virtud del presente Reglamento debe garantizarse mediante multas sancionadoras y multas coercitivas (Cdo. 144)
218. Ambos designados por la Comisión como plataformas de muy gran tamaño el 25 de abril de 2023 (*vid.* nota n.º 187).
219. Con fecha 30 de abril de 2024. Acceso al comunicado de prensa sobre la incoación de este procedimiento https://ec.europa.eu/commission/presscorner/detail/en/

Comisión abordan las políticas y prácticas de Meta (plataformas Facebook e Instagram) relativas a la publicidad engañosa y al contenido político en sus servicios. También se refieren a la falta de disponibilidad de un discurso cívico efectivo y de un instrumento de seguimiento electoral de terceros en el marco de las elecciones al Parlamento Europeo, en el contexto de la eliminación por parte de Meta de su herramienta de información pública en tiempo real *CrowdTangh*[220] sin que exista una herramienta de sustitución adecuada[221]. A esto se le une el hecho de que la Comisión sospecha que el mecanismo para señalar contenidos ilícitos en los servicios de estas plataformas ("*Notice-and Action*"), así como los mecanismos internos de recurso y reclamación de los usuarios, no cumplen los requisitos de la DSA. Además de la existencia de deficiencias en la prestación de acceso de *Meta* a los datos públicamente disponibles a los investigadores. La incoación del procedimiento formal se fundamenta en varios elementos: un análisis preliminar del informe de evaluación de riesgos enviado por *Meta* en septiembre de 2023; en las respuestas de Meta a las distintas solicitudes formales de información de la Comisión (sobre contenidos ilícitos y desinformación[222], acceso

---

ip_24_2373 En esa misma fecha, la Comisión puso en marcha una herramienta de denuncia de irregularidades para la Ley de Servicios Digitales (https://digital-services-act-whistleblower.integrityline.app/). La herramienta *DSA Whistleblower Tool* ofrece a las personas con información privilegiada una vía segura y protegida por la privacidad para compartir presentaciones anónimas o atribuidas de prácticas nocivas por parte de la muy grandes plataformas y motores de búsqueda a la Comisión Europea.

220. Se trataba de una herramienta de Meta, adquirida en 2016, que durante años ha servido con efectividad para medir la viralidad de los contenidos en las dos plataformas (Instagram y Facebook), lo que permitía a la sociedad civil, a la academia y a los periodistas para investigar la difusión de narrativas de desinformación y discursos problemáticos en estas redes y que desde agosto de 2024 ya no está en funcionamiento. Meta desarrolló este recurso como parte de sus obligaciones impuestas por la DSA al operar en la UE, en particular, para cumplir con el deber de ofrecer acceso a datos a investigadores independientes para detectar y comprender riesgos sistémicos dentro de la UE y la eficacia de las medidas tomadas por las plataformas para mitigarlos.

221. Por parte de Meta se sostiene que la clausura de *CrowdTangle* puede ser compensada con la apertura de su Biblioteca de Contenidos, una herramienta para ofrecer acceso casi en tiempo real a contenido público de páginas, publicaciones, grupos y eventos en Facebook, así como de cuentas de creadores de contenido y de negocio en Instagram. Según la compañía, estos datos pueden ser consultados a través de una interfaz gráfica o de la API. No parece que esta herramienta convenza como sustitución de la anterior por las restricciones de accesos a la información que se impone para acceder a esa Biblioteca según sus términos (https://about.fb.com/news/2023/11/new-tools-to-support-independent-research/?ref=platformer.news)

222. https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-0

a los datos[223], suscripción a la política de ausencia de anuncios[224] y sobre los riesgos del uso de IA generativa[225]); en informes de acceso público[226] y en el propio análisis de la Comisión.

El vigente procedimiento se centra en la investigación en los cuatro ámbitos concretos. En primer lugar, en la publicidad engañosa y desinformación. La Comisión sospecha que *Meta* no cumple las obligaciones de la DSA relacionadas con la lucha contra la difusión de anuncios engañosos, campañas de desinformación y comportamientos no auténticos coordinados en la UE. Sin duda la proliferación de este tipo de contenidos puede suponer un riesgo para el discurso cívico, los procesos electorales y los derechos fundamentales, así como para la protección de los consumidores; lo que justifica la supervisión e investigación iniciada. En segundo lugar, la Comisión se centra en la visibilidad del contenido político en las dos redes sociales. La Comisión sospecha que la política de Meta vinculada al "enfoque del contenido político", que destituye el contenido político en los sistemas de recomendación de *Instagram* y *Facebook*, incluidas sus fuentes (a través de sistemas algorítmicos), no cumple las obligaciones de la DSA. En este sentido, la investigación se focalizará en la compatibilidad de esta política con las obligaciones de transparencia y reparación de los usuarios, así como con los requisitos para evaluar y mitigar los riesgos para el discurso cívico y los procesos electorales. En tercer lugar, se analiza la falta de disponibilidad de un discurso cívico efectivo de terceros en tiempo real y de una herramienta de seguimiento electoral (con la eliminación de la herramienta "*CrowdTangh*"), en el marco de las ya pasadas elecciones al Parlamento Europeo y otras elecciones en varios Estados miembros que tendrán lugar a corto y medio plazo[227]; siendo estas herramientas (y

223. https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under

224. Nota de prensa sobre la solicitud de información por la Comisión disponible en https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-1

225. Puede consultarse la nota de prensa sobre la solicitud de información en https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-generative-ai-risks-6-very-large-online-platforms-and-2-very

226. Informes que pueden consultarse en la página web de la Comisión Europea "DSA Transparency Database" (https://transparency.dsa.ec.europa.eu

227. En el momento de la incoación del procedimiento Meta se encontraba en proceso de la eliminación de la herramienta de información pública *CrowdTangh que* permitía el seguimiento de las elecciones en tiempo real por parte de investigadores, periodistas y la sociedad civil, también a través de cuadros de indicadores visuales en directo, sin una sustitución adecuada. *Vid*. notas 220 y 221.

su acceso) esenciales en periodos de elecciones[228]. Por todo ello, se alzan justificadas sospechas para la Comisión, teniendo en cuenta este contexto particular, de que *Meta* no ha evaluado y mitigado adecuadamente, y con la diligencia exigida, los riesgos relacionados con los efectos de *Facebook* e *Instagram* en el discurso cívico y los procesos electorales y otros riesgos sistémicos vinculados a sus servicios[229]. En función de la información que se recabe por la Comisión se realizará la evaluación de la naturaleza y la inminencia de los daños. En este específico supuesto resultaba esencial la adopción por parte de Meta de las medidas necesarias para garantizar un control público efectivo en tiempo real de su servicio, proporcionando a los investigadores, periodistas y funcionarios electorales un acceso adecuado a las herramientas de seguimiento en tiempo real de los contenidos alojados en sus servicios (*Facebook* e *Instagram*) como se le ha solicitado[230]. En caso contrario, es más que previsible que las conclusiones de la Comisión sean de infracción de la DSA (con potenciales multas sancionadoras y/o coercitivas); al margen del derecho de la Comisión a adoptar medidas necesarias en caso de que las acciones adoptadas por Meta se consideren insuficientes. Por último, el mecanismo para señalar los contenidos ilícitos también es objeto de investigación por la Comisión en este procedimiento formal. Se sospecha que el sistema de notificación y acción de Meta, que permite a los usuarios notificar la presencia de contenidos ilícitos en sus servicios, no cumple las obligaciones de la DSA. Particularmente, parece que no se cumple con los requisitos que exigen que este mecanismo debe ser de fácil acceso y uso. Asimismo, está bajo investigación el sistema interno de tramitación de reclamaciones para los usuarios contra las decisiones de moderación de contenidos adoptadas por ambas plataformas (para verificar si es válido y eficaz a los efectos propuestos).

228. Con épocas de elecciones debe ampliarse el acceso a dichas herramientas, como así se refleja en las Directrices de la Comisión para los proveedores de plataformas en línea de muy gran tamaño sobre los riesgos sistémicos para los procesos electorales. A las que dedicaremos el siguiente apartado.

229. Esta no es una cuestión baladí, dado el alcance de las plataformas de Meta en la UE (que representan más de 250 millones de usuarios activos mensuales), en un contexto de procesos electorales sucesivos. La vigente situación de las redes podría dar lugar a daños al discurso cívico y a los procesos electorales en relación con las capacidades de rastreo de la desinformación y la desinformación, la identificación de la injerencia y la supresión de los votantes, y la transparencia general en tiempo real proporcionada a los verificadores de datos, a los periodistas y a otras partes interesadas electorales pertinentes.

230. La comisión emitió solicitud de información, tras la incoación de procedimiento formal, para que *Meta* comunique en el plazo de 5 días laborables las medidas correctoras adoptadas a tal efecto.

Si tras la investigación se demuestran los extremos que la Comisión sospecha, estos incumplimientos constituirían infracciones de los artículos 14 (1), 16 (1), 16 (5), 16 (6), 17 (1), 20 (1), 20 (3), 24 (5), 25 (1), 34 (1), 34 (2), 35 (1) y 40 (12) de la DSA, con las consecuencias ya señaladas en los casos anteriores analizados: posibles multas coercitivas y sancionadoras en su caso, tras la conclusión de todas las fases en este procedimiento de e ejecución.

51. Por último, haremos referencia a una importante decisión de política interna adoptada por la empresa *Meta* relativa a la eliminación de su sistema de verificación de contenidos vinculado a sus servicios digitales de intermediación, sustituyéndolo por un sistema de notas de la comunidad (*Community notes*)[231], siguiendo la estela de la red *X*. Si bien por el momento esta decisión solo afecta a los servicios prestados en EEUU, nada impide que se extienda esta decisión al mercado interior, por lo que habría que analizar si estas medias sustitutivas de "notas de Comunidad" cumplen con los requisitos exigidos por la DSA para los muy grandes prestadores de plataformas en línea; en especial para cumplimiento de las obligaciones de control y mitigación de riesgos sistémicos. El actual sistema de verificación de contenidos (moderación) que opera en *Meta* dentro de la UE (y hasta el momento en EEUU) es un sistema híbrido[232] que se articula a través del recurso a la IA (sistemas algorítmicos) y verificación humana (socios acreditados[233]). Según lo manifestado por el fundador de *Meta*, a partir de ahora en relación con los servicios de intermediación prestados en EEUU se elimina el recurso a los verificadores de datos, que se sustituyen por notas comunitarias, y se endurecen los filtros antes de eliminar los contenidos publicados para evitar la censura. El nuevo modelo de notas de la comunidad (en inglés, *Community Notes*) permitirá que los usuarios de las redes *Facebook* e *Instagram* indiquen qué publicaciones pueden parecer potencialmente engañosas y que requieren de más contexto —de esta manera la lucha contra la eventual desinformación queda en manos de los propios usuarios—. En el sistema anterior de verificación, esta labor era exclusivamente realizada por expertos y por organizaciones independien-

231. La empresa Meta anunció al inicio del año 2025 que eliminaba su sistema de verificación de datos por terceros en Estados Unidos. Este anuncio fue realizado por el propio fundador de la empresa, Zuck Zuckerberg, a través de su cuenta en la reda Instagram el día 8 de enero. Esta decisión se justifica en palabras del Zuckerberg por el "panorama político y social cambiante y un deseo de abrazar la libertad de expresión". En consecuencia, se anuncia un ajuste de los filtros "para que requieran mucha más confianza antes de eliminar el contenido". Acceso a la declaración completa en https://www.instagram.com/reel/DEhf2uTJUs0/?utm_source=ig_embed

232. *Vid*. Nota 156.

233. Entre otros la entidad *Check Your Fact.*

tes de comprobación de datos (socios acreditados). Lo que se pretende por la entidad multinacional es primar la libertad de expresión en sus redes sociales, manifestando los errores que en control de contenidos ilícitos se han constatado con el sistema de verificación existente, con el consecuente peligro de censura que esto conduce. Se confirma que sólo se continuará con la moderación del contenido cuando la información esté relacionada con drogas, terrorismo y explotación infantil[234]. Nada se dice sobre el control vinculado a la desinformación y la posible incidencia en el discurso cívico y los procesos electorales, cuya responsabilidad se deja en definitiva a la decisión de los propios usuarios a través de esas "notas". Esta aproximación eventualmente se justificaría con ese objetivo manifestado por este gigante tecnológico de garantizar la libertad de expresión en estos espacios para sus usuarios digitales, eliminando la presunción de condición de fuente de información que a estas plataformas se les atribuye. De esta manera se trataría de recuperar la esencia originaria de estas plataformas, como un espacio en línea de intercambio de opiniones y de libertad de expresión de los usuarios digitales; dejando en manos de los propios usuarios los contenidos que quieren consumir mediante ese "control" a través de las notas de comunidad —lo que en última instancia, se traduce en que el control de riesgos, y consecuente lucha contra la desinformación, recae igualmente en manos de los usuarios—. Ante esta decisión de la multinacional, la Comisión Europea ya ha avisado a *Meta* de que para los servicios que presta en la UE debe cumplir con las obligaciones impuestas por la DSA. Estas obligaciones exigen que antes de implementar funcionalidades que puedan tener un impacto crítico en los riesgos sistémicos, las plataformas en línea de gran tamaño deben realizar una evaluación de riesgos y presentar un informe a los servicios de la Comisión[235]. Es posible aventurar que por esta multinacional finalmente se adopte también en Europa esta política interna, en términos análogos a la red *X* que, recordemos está bajo investigación formal por esta y otras cuestiones. Esto supondría añadir otro factor a la investigación que por la comisión se está llevando a cabo en relación con las dos plataformas de Meta, específicamente en el contexto de la lucha contra la desinformación en el marco de los procesos electorales dentro de la UE.

234. Tal y como se desprende de la declaración del fundador https://www.instagram.com/reel/DEhf2uTJUs0/?utm_source=ig_embed

235. Como ha recordado ha recordado el portavoz de la Comisión Europea de soberanía tecnológica, Thomas Regnier. Información obtenida de la noticia https://www.rtve.es/noticias/20250107/meta-abandona-sistema-verificacion-datos-por-terceros-estados-unidos/16397475.shtml

2.2. Normas de autorregulación de las plataforma para hacer frente a la desinformación

52. La desinformación se percibe desde las instituciones europeas como un riesgo muy significativo contra el que se debe luchar, particularmente en el entorno digital por su potencial alcance global (dentro de esa pretendida soberanía digital). La desinformación perjudica a la propia sociedad de muchas formas: erosionando la confianza en las instituciones y en los medios de comunicación; poniendo en peligro los procesos electorales; obstaculizando la capacidad de los ciudadanos para tomar decisiones con conocimiento de causa, y menoscabando su libertad de expresión[236]. En particular, para la UE la desinformación se descubre como amenaza creciente para las democracias europeas. En este contexto, las normas de autorregulación de los principales agentes involucrados (muy grandes plataformas digitales y motores de búsqueda en lo que nos concierne) manifiestan especial relevancia para hacer frente a este riesgo; así se refleja en la normativa europea, como en la DSA, y las iniciativas presentadas en este ámbito en la UE, en especial, por la Comisión Europea. Nos centraremos, por razón de espacio, brevemente en los Códigos de buenas prácticas en materia de desinformación y en las Directrices para reforzar el vigente Código de Buenas Prácticas en materia de Desinformación, como marco de autorregulación esencial para las muy grandes plataformas digitales y buscadores[237].

53. En 2018 se estableció por primera vez un Código de buenas prácticas para las plataformas en línea, las asociaciones comerciales y los principales agentes del sector de la publicidad, que les comprometió —a los 16 firmantes[238]— a frenar la desinformación y mejorar sus políticas en línea. Con

---

236. Estas son las razones manifestadas por la Comisión europea para justificar la necesidad de reforzar el ´Código de buenas prácticas en materia de desinformación. Información obtenida de la página web de la comisión: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_es?s=09#un-c%C3%B3digo-de-buenas-pr%C3%A1cticas-en-materia-de-desinformaci%C3%B3n-reforzado

237. Un análisis cronológico de las distintas acciones de las acciones de la UE contra la desinformación, entre las que se encuentra la DSA, por el Observatorio Europeo de los Medios de Comunicación Digitales y los centros nacionales de este observatorio, puede verse en https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_es?s=09#un-c%C3%B3digo-de-buenas-pr%C3%A1cticas-en-materia-de-desinformaci%C3%B3n-reforzado

238. El Código de buenas prácticas fue firmado en octubre de 2018 por las plataformas en línea *Facebook, Google, Twitter y Mozilla*, así como por anunciantes y otros agentes

este instrumento por primera vez en el mundo la industria digital aceptó, de manera voluntaria, estándares de autorregulación para combatir la desinformación[239]. La finalidad de este Código era alcanzar mediante la autorregulación, los objetivos establecidos en la Comunicación de la Comisión presentada en abril de 2018[240], estableciendo 21 compromisos en diferentes ámbitos, que van desde la transparencia en la publicidad política hasta la desmonetización de los proveedores de desinformación[241]. En particular, sobre los procesos electorales, entre enero y mayo de 2019, la Comisión llevó a cabo un seguimiento específico de la aplicación de los compromisos asumidos por *Facebook, Google* y *Twitter* (actual *X*) a través de este Código, con especial relevancia para la integridad de las elecciones al Parlamento Europeo[242]. Este código de conducta se ha revelado como una herramienta innovadora para garantizar una mayor transparencia y rendición de cuentas de las plataformas en línea, así como para proporcionar un marco estructurado para el seguimiento y la mejora de las políticas de las plataformas en materia de desinformación[243]. Asimismo, ha demostrado ser muy útil también para supervisar y garantizar la rendición de cuentas de las acciones de los firmantes para limitar el impacto de la desinformación (en particular

---

del sector de la publicidad. *Microsoft* se adhirió en mayo de 2019, mientras que *TikTok* firmó el Código en junio de 2020.

239. El texto íntegro del Código de 2018 (*EU Code of Practice on Disinformation*) en https://ec.europa.eu/newsroom/dae/redirection/document/87534

240. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, para luchar contra la desinformación en línea: un enfoque europeo. COM/2018/236 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236)

241. En especial destacan los compromisos sobre el análisis de la colocación de los anuncios; la transparencia de la publicidad política y temática; la integridad de los servicios; la capacitación de los consumidores; la capacitación de los verificadores de datos y los investigadores y medición de la eficacia del Código.

242. En octubre de 2019, tras un año de aplicación del Código, se publicó un informe de autoevaluación de los firmantes. Acceso a este informe y resto de informes anuales de los firmantes (autoevaluaciones) en https://digital-strategy.ec.europa.eu/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

243. A la luz de la evaluación del Código presentada por la Comisión en septiembre de 2020. La evaluación puso de manifiesto que el Código proporcionó un valioso marco para un diálogo estructurado entre plataformas en línea y garantizó una mayor transparencia y rendición de cuentas de sus políticas en materia de desinformación. También dio lugar a acciones concretas y cambios políticos por parte de las partes interesadas pertinentes para ayudar a contrarrestar la desinformación. Documento de trabajo de los servicios de la Comisión SWD (2020)180 Final — Evaluación del Código de prácticas sobre desinformación (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212).

en momentos complicados como la pandemia COVID-19[244]). Sin embargo, la evaluación también puso de manifiesto una serie de lagunas y deficiencias importantes. Como consecuencia, y tal como se anunció en el Plan de Acción para la Democracia Europea, la Comisión publicó unas directrices en mayo de 2021[245] sobre el refuerzo del Código, en las que indicaba cómo los signatarios debían abordar las deficiencias para convertirlo en una herramienta sólida, eficiente y flexible para luchar contra la desinformación. Seguidamente, como consecuencia, se puso en marcha un proceso de revisión que concluyo con el Código de prácticas sobre desinformación de 2022[246]. El Código de buenas prácticas contra la desinformación de 2022 supone la autorregulación para plataformas en línea de muy gran tamaño en el marco de la DSA para combatir este riesgo sistémico (así los grandes gigantes tecnológicos pueden adherirse a estos estándares de autorregulación reforzados para combatirla). Este Código reforzado de 2022 cuenta con 34 firmantes y está integrado por 44 compromisos y 128 medidas específicas en distintos ámbitos, tales como: desmonetizar la difusión de desinformación; garantizar la transparencia de la publicidad política; empoderar a los usuarios[247]; mejorar la cooperación con los verificadores de datos; y proporcionar a los investigadores un mejor acceso a los datos[248]. Específicamente para combatir la desinformación en el contexto de procesos electorales se recoge el compromiso de los signatarios de cooperar y coordinar su trabajo durante las elecciones, cuando la amena-

244. Durante la crisis del coronavirus, las plataformas informaron mensualmente a la Comisión facilitándole una visión general de sus acciones para promover contenidos fidedignos, mejorar la sensibilización de los usuarios, degradar los contenidos nocivos o tomar medidas contra ellos, e identificar los flujos de publicidad relacionados con la desinformación relativa al coronavirus.
Se pueden consultar los primeros informes de referencia — Programa de seguimiento de la lucha contra la desinformación sobre la COVID-19, presentados por los distintos firmantes en https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme

245. Orientaciones de la Comisión Europea sobre el fortalecimiento del Código de buenas prácticas en materia de desinformación (COM(2021) 262 final). Brussels, 26.5.2021.

246. Su proceso de revisión se puso en marcha en junio de 2021 y, tras la firma y presentación del Código revisado el 16 de junio de 2022. Los signatarios del Código de 2018, junto con una amplia gama de posibles signatarios, participaron en el proceso de revisión que dio lugar al Código reforzado presentado a la Comisión. texto íntegro del nuevo código de 2022 en https://ec.europa.eu/newsroom/dae/redirection/document/87585

247. Comprometiéndose a la ampliación y refuerzo de las herramientas que capacitan a los usuarios, por ejemplo para detectar y señalar contenidos falsos o engañosos. Dentro de los sistemas *notice-and-action* del art. 16 DSA.

248. En profundidad sobre principales acciones recogidas en este Código de 2022 y su relación con la DSA *vid*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

za de las campañas de desinformación es especialmente elevada. Según lo previsto en el Código, los signatarios establecieron un sistema de respuesta rápida para garantizar una cooperación rápida y eficaz entre plataformas, organizaciones de la sociedad civil y verificadores de datos durante los períodos electorales, operativo para las elecciones al Parlamento Europeo de junio de 2024[249]. Dada la pretendida vocación de futuro de este Código, los signatarios acordaron establecer un marco para una mayor colaboración a través de un grupo de trabajo permanente. El Código también viene con un marco de seguimiento reforzado basado en elementos de información cualitativa e indicadores de nivel de servicio que miden la eficacia de su aplicación. Los signatarios han creado un Centro de Transparencia, donde se publican las políticas que ponen en marcha para implementar sus compromisos y que se actualiza periódicamente con los datos pertinentes[250].

Este Código de buenas prácticas reforzado forma parte de un marco regulador más amplio para los operadores digitales vinculados, en combinación con la legislación sobre transparencia y segmentación de la publicidad política y la DSA. Para los signatarios que son plataformas en línea de muy gran tamaño y motores de búsqueda, este Código pretende convertirse en una medida de mitigación de riesgos sistémicos y un Código de Conducta a luz de la DSA. La virtualidad de este instrumento para el cumplimiento suficiente de las obligaciones impuestas a estos grandes operadores digitales por la DSA se verificará por las autoridades nacionales y europeas.

54. Por último, y como complemento a lo anterior, dentro de ese marco de corregulación[251] para las muy grandes plataformas y motores de búsqueda para la gestión y mitigación de la desinformación, se hará referencia a las Directrices emitidas por la Comisión el pasado abril de 2024[252] dirigidas a estos gigantes digitales, para la reducción de los riesgos sistémicos en los

249. En marzo de 2024, los signatarios del Código de buenas prácticas sobre desinformación informaron sobre las medidas que estaban adoptando o planeaban adoptar para proteger las elecciones al Parlamento Europeo. Estas medidas específicas están disponibles en secciones específicas de sus informes que se pueden encontrar en https://disinfocode.eu/eu-elections-2024/

250. Cuya página web es https://disinfocode.eu/

251. La Comisión indica que estas directrices deben considerarse en el marco del apoyo a los proveedores de plataformas en línea de muy gran tamaño y plataformas en línea de muy gran tamaño para garantizar el cumplimiento de la obligación establecida en el art. 35 de la DSA respecto a los riesgos en los procesos electorales. Tal y como aparece en la web oficial de la UE (https://digital-strategy.ec.europa.eu/es/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes).

252. Comunicación de la Comisión. Directrices de la Comisión para los proveedores de plataformas en línea de gran tamaño y motores de búsqueda en línea de gran tamaño

procesos electorales[253]. No obstante, como premisa se recuerda que estos operadores digitales que prestan servicios dentro de la UE, además de la obligación de establecer medidas de mitigación razonables, proporcionadas y eficaces para los riesgos relacionados con los procesos electorales, de conformidad con el artículo 35 DSA (a cuyo cumplimiento se vinculan estas Directrices), deben cumplir todas las demás obligaciones legales recogidas en este instrumento que puedan ser pertinentes[254]. En este documento la Comisión ofrece orientaciones destinadas a apoyar las plataformas en línea y buscadores de muy gran tamaño para garantizar que cumplen su obligación de reducir los riesgos específicos vinculados a los procesos electorales. Entre los riesgos señalados por la Comisión (de manera no exhaustiva), se encuentra la proliferación de la incitación ilegal al odio en internet, las amenazas relacionadas con la manipulación de la información y la injerencia por parte de agentes extranjeros[255]; así como el fenómeno más amplio de la desinformación, la difusión de contenidos extremistas (violentos) y de contenidos destinados a la radicalización de las personas, y la difusión de contenidos generados mediante nuevas tecnologías, como la IA generativa[256]. En el marco de procesos electorales, los riesgos sistémicos también pueden manifestarse mediante la amplificación y, potencialmente, la difusión rápida y amplia de contenidos ilícitos (con arreglo a la legislación europea o de los Estados miembros); como son, por ejemplo, amenazas, contenidos extremistas y terroristas violentos, incitación ilegal al odio o acoso en línea contra candidatos o cargos políticos, periodistas, trabajadores electorales u otras personas participantes en el proceso electoral[257]. El ámbito de aplicación subjetivo de estas Directrices se concreta en las plataformas en línea y motores de búsqueda de muy gran tamaño cuyos servicios estén expuestos a efectos negativos reales o previsibles en los procesos electorales derivados del diseño, el funcionamiento y el uso de dichos servicios en el sentido del art. 34 de la DSA. En consecuencia, estos prestadores deben aplicar estas directrices (y las medidas específicas en ellas recogidas) a los procesos electorales en los Estados miembros, incluidas las elecciones nacionales y las

---

sobre la mitigación de los riesgos sistémicos para los procesos electorales de conformidad con el artículo 35, apartado 3, del Reglamento (UE) 2022/2065. C/2024/2537.

253. Estas directrices se basan en una serie de diálogos sobre la preparación en materia de integridad electoral mantenidos por la Comisión con varios prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño tras la entrada en vigor de la DSA.
254. *Vid. Supra* Apdo. III. 1.
255. *FIMI*, por sus siglas en inglés.
256. *Vid*. numeral 3 del punto 1.1 de las Directrices (Finalidad y base jurídica).
257. *Vid*. numeral 7 del punto 1.1 de las Directrices.

elecciones institucionales (en su momento respecto al Parlamento Europeo por las fechas de publicación). Las medidas previstas en este documento abarcan los periodos preelectoral, electoral y postelectoral. Asimismo, deben aplicarse medidas de reducción a las elecciones o referendos regionales y locales, en caso de que las evaluaciones de riesgos concluyan que existen efectos negativos reales o previsibles para estos procesos electorales. Concretamente, las Directrices recogen una serie de medidas orientadas a distintos ámbitos: el refuerzo de los procesos internos de las propias plataformas; la reducción de los riesgos sistémicos para los procesos electorales y unas medidas específicas de reducción de riesgos relacionadas con la IA generativa[258]. Por razón de espacio y coherencia con el objeto de estudio, nos limitaremos a referirnos a estas últimas[259].

Como punto de partida, se reconoce por la Comisión que el uso de IA generativa puede dar lugar a riesgos sistémicos específicos en contextos electorales. En particular, cabe hacer uso abusivo de la IA generativa para inducir a error a los votantes o manipular los procesos electorales mediante la creación y difusión de contenidos sintéticos no auténticos, sesgados y engañosos (textos, imágenes, audios y contenidos audiovisuales como vídeos) en relación con actores políticos, la representación falsa de acontecimientos, encuestas electorales, contextos o narrativas. Los sistemas de IA generativa también pueden producir información incorrecta, incoherente o inventada, lo que se conoce como "alucinaciones", que tergiversan la realidad y pueden inducir a error a los votantes[260]. La Comisión vincula expresamente estos elementos de riesgo con las obligaciones previstas en el Reglamento IA[261] para los proveedores de modelos de IA de uso general, incluida la IA generativa. En particular, los requisitos para el etiquetado de las "ultrafalsificaciones"[262] y los que exigen a los proveedores de sistemas de IA generativa que utilicen soluciones técnicas de vanguardia para garantizar que los contenidos creados mediante IA generativa estén marcados en un formato legible por máquina y sean identificables como tales —esto permitirá su detección por parte de las muy grandes plataformas y buscadores—.

258. Un análisis pormenorizado de estas directrices, en particular de las distintas medidas en C.B. FERNÁNDEZ, "La Comisión emite unas directrices dirigidas a las plataformas y motores de búsqueda en línea de muy gran tamaño, para la reducción de los riesgos sistémicos en los procesos electorales", *La ley,* 26-4-2024.
259. A las que se dedica el punto 3.3 (Medidas de mitigación vinculadas a la IA generativa), apdos. 36-42.
260. *Cfr*. Apdo. 36 de las Directrices.
261. *Vid. supra* Apdo. II.1.
262. O *Deep fakes*. Se trata de información que puede parecer veraz y real para las personas pero que es falsa (o ha sido manipulada).

En consecuencia, en estas Directrices se recomienda que estos operadores digitales adapten sus políticas al Reglamento de la IA antes de su entrada en vigor, de conformidad con el Pacto sobre la IA[263].

Asimismo, se establece que estos grandes prestadores de servicios deben aplicar las medidas de reducción relacionadas con la IA generativa recogidas en las Directrices, en la medida en que sean técnicamente factibles, con especial atención a la incidencia de dichas medidas en los derechos fundamentales protegidos por la CDFUE. De esta suerte, la Comisión recomienda que las plataformas en línea y motores de búsqueda de muy gran tamaño cuyos servicios puedan utilizarse para la creación de contenidos de IA generativa engañosos, sesgados, falsos o que induzcan a error cuenten, en la medida en que sea técnicamente factible, y de acuerdo con el estado actual de la técnica, con medidas de reducción del riesgo, como son: garantizar que el contenido de IA generativa y otros tipos de medios sintéticos y manipulados sean detectables; procurar garantizar que la información generada por los sistemas de IA se base, en la medida de lo posible, en fuentes fiables en el contexto electoral (como la información oficial de las autoridades electorales pertinentes), y que las citas o referencias hechas por el sistema a fuentes externas sean exactas y no tergiversen el contenido citado, limitando así los efectos de las alucinaciones; advertir a los usuarios de posibles errores en los contenidos creados por sistemas de IA generativa y sugerirles que consulten fuentes autorizadas para comprobar la veracidad de dicha información; así como establecer salvaguardias para evitar la creación de contenidos falsos que puedan tener un gran potencial para influir en el comportamiento de los usuarios. La Comisión recomienda también que las plataformas cooperen y compartan información sobre contenidos engañosos con verificadores de datos a fin de garantizar que se minimice el riesgo de amplificación en otras redes. En consecuencia, se puede deducir que los mecanismos de verificación de contenidos (moderación proactiva) de las plataformas y motores de búsqueda no deben de dejarse exclusivamente en manos de los sistemas de IA (sistemas algorítmicos automatizados) sino que se al menos sea métodos híbridos con verificadores de datos.

Se pone especial enfoque en la necesidad de que se adopten por estos operadores las medidas que sean necesarias y adecuadas[264] para que los usuarios puedan distinguir las imágenes, los audios o vídeos sintéticos o

263. *Vid*. nota 23.

264. Como por ejemplo, el etiquetado, que se manifiestas de utilidad a los efectos de destacar estos contenidos de manera efectiva, como se indica por la Comisión en la directrices. No se impone este mecanismo sino que se deja a elección de las plataformas el medio

manipulados, que se asemejen sensiblemente a personas, objetos, lugares, entidades o eventos reales, que muestren como reales acontecimientos que no se produjeron o que tergiversen los acontecimientos, y que puedan parecer, falsamente, auténticos o veraces para los usuarios[265]. También las recomendaciones se focalizan en las herramientas que deben facilitarse por las plataformas a sus usuarios para que estos puedan identificar aquellos contenidos generados por la IA que distribuyen a través de sus servicios. Así, la Comisión recomienda que se proporcione a los usuarios interfaces y herramientas estándar y fáciles de utilizar para añadir etiquetas a los contenidos generados por la IA[266]. Debiendo las plataformas probar la eficacia de dichas etiquetas antes de empezar a mostrarlas, así como adaptarlas y mejorarlas en función de las observaciones realizadas y de la experiencia. También las medidas propuestas por la Comisión, vinculadas a la IA generativa, se dirigen a los sistemas de publicidad. La Comisión recomienda a las plataformas adaptar sus sistemas de publicidad, por ejemplo ofreciendo a los anunciantes opciones para etiquetar claramente los contenidos creados con IA generativa en la publicidad o en las publicaciones promocionadas, y que exijan en su política publicitaria que estas etiquetas se utilicen cuando el anuncio incluya contenidos de IA generativa.

En consecuencia, para hacer cumplir estas políticas, las plataformas en línea y motores deben adaptar sus procesos de moderación de contenidos y sistemas algorítmicos de manera que se detecten contenidos de IA generados o manipulados mediante marcas de agua, identificaciones de metadatos, métodos criptográficos para demostrar la procedencia y autenticidad de los contenidos, métodos de registro, impresiones dactilares u otras técnicas. En este contexto, las muy grandes plataformas y motores de búsqueda en línea deben cooperar con los proveedores de sistemas de IA generativa y aplicar las medidas más avanzadas para garantizar que dichas marcas de agua, identificaciones de metadatos, métodos criptográficos para demostrar la procedencia y autenticidad de los contenidos, métodos de registro, impresiones dactilares u otras técnicas se detecten de manera fiable y eficaz; también se les recomienda apoyar las innovaciones en las nuevas tecnologías a fin de mejorar la eficacia y la interoperabilidad de dichas herramientas.

---

a utilizar siempre que se cumpla con la función y objetivo buscado: evitar la confusión para los usuarios digitales mitigando el riesgo de desinformación.

265. Lo que se conocen como ultrafalsificaciones o *Deep fakes*.

266. Para etiquetar contenidos de IA generativa, la Comisión recomienda que las plataformas apliquen etiquetas eficientes y fácilmente reconocibles por los usuarios, teniendo en cuenta aspectos como los gráficos, la posición y el momento de la aplicación, basándose en la investigación científica sobre la eficacia de las etiquetas.

55. A la luz de lo referido, la presencia de la IA vinculada a los servicios digitales de las plataformas (en sentido amplio) dentro de la UE, en la particular materia objeto de estudio, puede conllevar una corregulación significativa en la prestación de sus servicios. De esta suerte, cuando los servicios de estos operadores no se limitan a la intermediación sino que puedan considerarse como proveedores de sistemas de IA (ordinariamente generativa) para sus usuarios, les será de aplicación no solo las obligaciones impuestas por la DSA, sino las recogidas por el Reglamentos de la IA, y especialmente para la mitigación del riesgo de desinformación vinculada a los procesos electorales, las Directrices de 2024 (además de la autorregulación en la forma de códigos de conducta que se hayan suscrito).

IV. CONCLUSIONES

56. La utilización de la IA en general (y de la IA generativa en particular) crea riesgos que pueden concluir en responsabilidad por daños, típicamente no materiales, que habrá que determinar en qué casos y frente a quién/es puede exigirse en función de la normativa aplicable (fundamentalmente europea, si es que opera dentro de la UE). La presencia de la IA vinculada a la prestación de servicios digitales, típicamente de intermediación, de las (muy grandes) plataformas y motores de búsqueda dentro de la UE, establece un marco jurídico de concurrencia normativa dispar en función de qué tipo de IA se trate, cómo se utiliza y por quién. Este marco jurídico determinará el conjunto de obligaciones legales —vinculadas a la diligencia debida esencialmente— que deben cumplir los implicados (frente al riesgo que su uso genera), así como su régimen de responsabilidad frente a la generación de eventuales daños.

57. En este entorno, cabe referir la incidencia de la IA desde dos perspectivas distintas en relación con la prestación de servicios realizada por las plataformas digitales y motores de búsqueda. Por un lado, el uso de la IA en sentido amplio, que comprende los sistemas algorítmicos de toma de decisiones automatizadas, que es utilizado típicamente por las muy grandes plataformas digitales y motores de búsqueda en su actividades tanto de moderación (sistemas de verificación) como de curación de contenidos (recomendación, incluida publicidad). En la medida que estos operadores digitales desarrollen su actividad dentro de la UE, deben someterse y cumplir con las obligaciones que la DSA impone. Desde esta perspectiva, el recurso de la IA coadyuva eficazmente en el objetivo de cumplir con las obligaciones de evaluación y mitigación de riesgos sistémicos vinculados a sus servicios, entre los que se encuentra la lucha contra los contenidos ilícitos

y la desinformación (obligaciones de diligencia debida que condicionan su régimen de exención de responsabilidad respecto de actos de terceros: sus usuarios). Los sistemas algorítmicos utilizados para verificación de datos permiten a las grandes plataformas dar una respuesta ágil y eficiente, especialmente ante contenidos potencialmente dañinos o que pueden volverse virales rápidamente, dado el elevado número de usuarios. No obstante, frente a esas evidentes ventajas del uso de la IA para esa labor de moderación, su operatividad no está exenta de controversias y desafíos. El control o moderación de contenidos impacta potencialmente en derechos fundamentales como es la libertad de expresión en el sentido más omnicomprensivo (ya que como consecuencia puede suponer una eventual censura del usuario digital). De esta suerte, la implementación de IA en la moderación de contenidos por las grandes plataformas y buscadores, con el fin crear entornos digitales más seguros (en cumplimiento de la normativa europea), requiere un equilibrio cuidadoso entre eficiencia en el cumplimiento de ese objetivo y la protección de derechos fundamentales implicados. Es por ello por lo que el ejercicio de esa labor debe realizarse de manera justa, equilibrada y transparente. La principal y esencial cuestión que plantea el uso de la IA para esta labor es que puede conducir a resultados equívocos o sesgados. Asimismo, la falta transparencia sobre el funcionamiento de los algoritmos sobre la toma de decisiones (automatizada) es una cuestión controvertida. Las mismas consideraciones caben extraerse prácticamente para la labor de curación y ofrecimiento de información personalizada a los usuarios (incluyendo publicidad dirigida) mediante el recurso a sistemas algorítmicos; con el riesgo en este caso además de las indeseadas "burbujas de filtro". Para tratar de mitigar resultados no deseados y no justificados (en equilibrio de esta necesaria labor de control de riesgos y garantía de derechos fundamentales), la DSA establece obligaciones de transparencia y rendición de cuentas para las grandes plataformas sobre sus prácticas de moderación y curación de contenidos, especialmente con el uso de la IA. Precisamente el cumplimiento de las obligaciones impuestas por la DSA para la evaluación y gestión de los riesgos sistémicos en el desarrollo de sus servicios están siendo objeto de especial investigación por las autoridades nacionales y europeas desde la entrada en aplicación de la norma. Destacan los procedimientos formales instados por la Comisión frente a muy conocidas redes, particularmente ante el riegos de desinformación potenciada y difundida en estos espacios en el marco de procesos electorales (vinculado especialmente a los sistemas algorítmicos utilizados)[267]. No puede obviarse el hecho de que las

267. La transparencia y la rendición de cuentas en relación con la moderación de contenidos y la publicidad constituyen el núcleo de la DSA y su seguimiento mediante la imposición de obligaciones sustantivas para las muy grandes plataformas digitales y

plataformas y los motores de búsqueda en línea se han convertido en lugares importantes para el debate público, la configuración de la opinión pública y el comportamiento de los votantes. En consecuencia, a estos operadores les es exigible una especial diligencia para llevar a cabo las evaluaciones de riesgos concretos y aplicar medidas de reducción del riesgo razonables, proporcionadas y eficaces, en particular para cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública. Desde esta perspectiva, la labor de moderación (proactiva) y curación de contenidos de las muy grandes plataformas digitales puede ser un mecanismo importante para la lucha contra la desinformación siempre que se utilicen herramientas no solo efectivas sino adecuadas. Las plataformas deben equilibrar la eficacia en la lucha contra la desinformación (en cumplimiento de sus obligaciones y con el objeto de no incurrir en responsabilidad y potenciales sanciones) con la protección de los derechos fundamentales de los usuarios y la transparencia en sus procesos de toma de decisiones. En definitiva, además de utilizar medias efectivas (como así resulta del recurso a la IA) éstas deben ser adecuadas; lo que parece que sólo con los sistemas de IA (aun plenamente transparentes) no puede garantizarse por los sesgos y equivocaciones que esta tecnología manifiesta en sus resultados[268]. En conclusión, cabe afirmar que las plataformas en línea son actores clave en la lucha contra la desinformación, y desde esta perspectiva el recurso a la IA es significativo (por su eficacia) pero debe controlarse y completarse. Por ello, el papel de estos agentes debe equilibrarse con una mayor transparencia, rendición de cuentas en el ejercicio de sus funciones y el cumplimiento de las obligaciones impuestas por la regulación (control), pero también mediante la colaboración (complemento) con otros sectores

---

motores de búsqueda que operen dentro de la UE ha justificado la incoación de varios procedimientos formales por parte de la Comisión frente a grandes tecnológicas. Estos procedimientos dan muestra de la firme intención de las instituciones europeas de supervisar las actividades que estos grandes operadores desarrollan dentro de la mercado interior y su adecuación a esta normativa. En particular, ante la amenaza o sospecha de incidencias externas que interfieran en procedimientos electorales dentro de la Unión, a través de los servicios digitales de las plataformas en línea, el compromiso es de actuar con rapidez y firmeza desde la Comisión, evaluando si se han vulnerado las disposiciones de la DSA que obligan a estos agentes a evaluar, controlar y mitigar estos supuestos como riesgo sistémico de sus servicios, para lo que deben todas ellas rendir cuentas.

268. Los objetivos a los que se debería orientar las políticas de control y administración de contenidos de las plataformas en relación con la IA son sencillos: hacer prevalecer la transparencia, combatir el sesgo, respetar la privacidad y mantener la supervisión humana junto con los sistemas de decisión automatizada. De esta forma no solo se conseguir aunaos resultados eficientes, sino también la defensa de los valores de integridad, autenticidad y confianza del usuario.

(pero tampoco de manera excluyente ni exclusiva por los posibles intereses en concurrencia), que podía incluir gobiernos junto a verificadores de hechos y la propia sociedad civil (por ejemplo, a través de las notas de comunidad).

Por otro lado, cabe referir el recurso a los sistemas de IA generativa para elaborar contenidos que se publiquen y difundan a través de los servicios en línea de estos operadores digitales (con potencial alcance global dado el número de usuarios de cierta plataformas y redes). Estos contenidos pueden ser ilícitos (desde el punto de vista jurídico, en atención al ordenamiento jurídico de referencia[269], o simplemente contrarios a las condiciones generales o términos de uso de la plataforma[270]); pero también pueden constituir información no deseada por el efecto negativo que pueden generar. En este último aspecto es donde encajarían los conocidos como bulos (*fake news* en su terminología en inglés), o incluso contenido que suponga manipulación de información real con el objetivo de desinformar (especialmente en contextos vinculados a procesos electorales), utilizando tecnología de IA para esas *ultrafalsificaciones* o *deepfakes*. De los contenidos no deseados puede generarse responsabilidad exigible, no solo frente a los autores materiales[271] sino eventualmente también a los que resulten responsables[272] de la IA utilizada (vinculado a las obligaciones impuestas por el Reglamento IA en función del nivel de riesgo o ante una eventual futura responsabilidad no contractual potencialmente exigible[273]), pero además frente a las plataformas a través de las cuales se difunde este contenido controvertido generado por IA. En

269. Legislaciones nacionales o normativa europea.
270. De ahí la relevancia de las Políticas internas del servicio digital, ya que estas no solo alcanzan a los usuarios en particular, sino que afectan (indirectamente) a la sociedad en su conjunto en la medida que, en última instancia, deciden qué contenidos se publican y difunden es su espacio y cómo (establecen el acceso y la visibilidad de la información en Internet), en función de unos algoritmos diseñados por estos operadores según sus intereses y fines particulares.
271. Fundamentalmente los usuarios que difunden los contenidos en las redes siempre que su comportamiento no esté tutelado por la libertad de expresión. Dejando al margen el régimen particular para los medios de comunicación en el ejercicio de la libertad de información; así como la posible responsabilidad de la editorial o titular del medio frente a los daños causados por los periodistas sujetos a su control.
272. En términos generales, los proveedores de esta tecnología en sentido amplio dentro de la UE, de conformidad con el Reglamento IA.
273. Si es que se demuestra el daño y la relación de causalidad, si encajara dentro el ámbito de la responsabilidad extracontractual por uso de la IA, en el contexto de una futura Directiva, si es que en algún momento vuelve a presentarse esta propuesta. Ahora bien, la operatividad de este futuro instrumento parece que en este ámbito queda en entredicho en los términos expuestos en el ahora texto retirado. *Vid.* conclusiones previas del Apdo. II.2.2.

este último aspecto, el marco jurídico aplicable para estos operadores digitales, que determina los mecanismos y medidas suficientes a adoptar para evitar responsabilidad, se configura actualmente no solo por la DSA (por las obligaciones impuestas por este instrumento, así como la normativa de autorregulación[274], asumida típicamente dentro de los códigos de conducta a la luz de este instrumento y directrices de desarrollo), pero también por el Reglamento de IA en caso de que puedan ostentar la condición de proveedores del sistema de IA generativo (como parte de sus servicios).

58. Toda vez que en la DSA nada se dice expresamente sobre la adopción de medidas de reducción de riesgos vinculados a la IA generativa por los grandes prestadores de servicios de intermediación[275], sería conveniente modificar esta norma en este aspecto. El objetivo sería introducir todos los supuestos de IA y riesgos vinculados a su uso (no sólo en la primera de las vertientes: la relativa a los sistemas algorítmicos en la moderación proactiva y sistemas de recomendación) y equiparar el contenido creado por sistemas de IA generativa a los contenidos generados por los usuarios de las plataformas digitales (que las utilizan para su difusión) a los efectos de que puedan aplicarse las medidas y mecanismos de control del contenido ilícito (no condicionar estas medidas a la condición de proveedor de los sistema de IA a la plataforma cuando sea parte de sus servicios). En definitiva, el marco jurídico en el ámbito de la soberanía digital es complejo para todos los operadores y sujetos implicados, en particular en esta materia específica, los resultados inciertos y la tecnología de IA sigue avanzando.

BIBLIOGRAFÍA

BARATA MIR, J.: "Libertad de expresión y moderación privada de contenidos", *Teorder*, 2022, núm. 32, pp. 88-107.

274. Para llevar a cabo evaluaciones de riesgos más frecuentes o específicas relacionadas con las funciones de los prestadores de servicios en línea que exige la DSA. En particular, cuando los riesgos se compartan entre plataformas en línea o motores de búsqueda en línea diferentes, deben colaborar con otros prestadores de servicios, por ejemplo, mediante la adopción de nuevos códigos de conducta o la suscripción a los ya existentes, u otras medidas de autorregulación. También deben sopesar medidas de concienciación, en especial cuando los riesgos estén relacionados con campañas de desinformación.

275. Dejando al margen la referencia específica a las medidas de mitigación vinculadas a la IA generativa en las Directrices de la Comisión de abril de 2024, dirigidas a las plataformas y motores de búsqueda en línea de muy gran tamaño, para la reducción de los riesgos sistémicos específicamente en los procesos electorales.

BARRIO ANDRÉS, M., "Consideraciones sobre el ámbito extraterritorial del Reglamento Europeo de Inteligencia Artificial", *Derecho Digital e Innovación. Digital Law and Innovation Review*, N.º 20, 2024.

BARRIO ANDRÉS, M. "El efecto Bruselas del Reglamento Europeo de inteligencia artificial", *OTROSÍ.: Revista del Colegio de Abogados de Madrid*, ISSN-e 2479-7197, N.º 2, 2024, pp. 47-48.

BERNASCONI, S., "Il ruolo del diritto internazionale privato e processuale nell'attuazione del 'pacchetto sui mercati e servizi digitali' (DMA&DSA)", *Rivista di diritto internazionale privato e processuale (RDIPP*), 4/2024, pp. 1184-1307.

CASTELLÓ PASTOR, J.J. "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea", Vol. 17, n.º 1 (marzo 2025), *CDT,* pp. 308-328.

CASTELLÓ PASTOR, J.J.: "Exoneración de responsabilidad de los prestadores de servicios de la información en la sección 230 de la *Communications Decency A*ct estadounidense", *Revista Aranzadi de derecho y nuevas tecnologías*, 2015, núm. 39, pp. 175-194.

CASTELLÓ PASTOR, J.J. *(Dir.), Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*), Aranzadi, 2024.

CORBERÁ MARTÍNEZ, J.: "Diseño y organización de interfaces en línea en el Reglamento de servicios digitales", en AA.VV.: *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2024, pp. 171-200.

CORDERO ÁLVAREZ, C.I., "El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro", en J.J. CASTELLÓ PASTOR (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105.

CREEL, K. Y HELLMAN, D.: "The Algorithmic Leviathan: Arbitrariness, Fairness, and Opportunity in Algorithmic Decision-Making Systems", *Canadian Journal of Philosophy*, 2022, vol. 52, pp. 26-43.

CRUZ ÁNGELES, J., "Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso", *CDT* (Octubre 2022), Vol. 14, N.º 2, pp. 294-318.

DOUEK, E.: "Content moderation as systems thinking", *Harvard Law Review*, 2022, vol. 136, pp. 526-607.

ELKIN-KOREN, N. Y MAAYAN P.: "Guarding the guardians: content moderation by online intermediaries and the rule of law", en AA.VV.: *Oxford Handbook of Online Intermediary Liability* (ed. por G. FROSIO), Oxford Academic, 2020, Chapter 34, pp. 669-678.

ELKIN-KOREN, N., "Contesting algorithms: restoring the public interest in content-removal AI", *Big Data & Society*, July 2020 (https://journals.sagepub.com/doi/full/10.1177/2053951720932296).

FELIU ÁLVAREZ SOTOMAYOR, S.: "Ámbito territorial y aplicación del principio del control en origen en el Reglamento UE de servicios digitales", en AA.VV. *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2024, pp. 41-64.

FERNÁNDEZ, C.B., "La Comisión emite unas directrices dirigidas a las plataformas y motores de búsqueda en línea de muy gran tamaño, para la reducción de los riesgos sistémicos en los procesos electorales", *La ley*, 26-4-2024.

GANESH, B. Y BRIGHT, J.: "Countering extremists on social media: challenges for strategic communication and content moderation", *Policy & Internet*, 2020, vol. 12, núm. 1, pp. 6-19.

GASCÓN MARCÉN, A.: "La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro", en AA.VV.: *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (Dir. por J.J. CASTELLÓ PASTOR), Aranzadi, 2021, pp. 133-160.

GILLESPIE, T.: "Content Moderation, AI, and the Question of Scale", *Big Data & Society*, agosto 2020 (https://journals.sagepub.com/doi/epub/10.1177/2053951720943234).

GILLESPIE, T.: *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media,* Yale University Press, New Haven, 2018.

G'SELL, F., "The Digital Services Act: A General Assessment", en *Content Regulation in the European Union. The Digital Services Act* (ed. A. UNGERN-STERNBERG (ed.), vol. 1, TRIER STUDIES ON DIGITAL LAW, pp. 85-118.

GRIMMELMANN, J.: "The virtues of moderation", *Yale Journal of Law & Technology*, 2015, vol. 17, n.º 42, pp. 43-109.

GRIMMELMANN, J.: "The structure of search engine Law", *Iowa Law Review*, 2007, vol. 93, n.º 1, pp. 1-63.

HACKER, P., ENGEL, A., MAUER, M., "Regulating ChatGPT and other Large Generative AI Models", *working paper*, disponible en https://arxiv.org/pdf/2302.02337 (Fecha de la consulta: 11 noviembre de 2024 2023), pp. 1-31, en esp. p. 16.

HOBOKEN, J., QUINTAIS, J., POORT, J. Y EIJK, N., "*Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report*", *Oficina de Publicaciones*, 2019, https://data.europa.eu/doi/10.2759/284542

KELLER, D.: "Inception Impact Assessment: Measures to Further Improve the Effectiveness of the Fight Against Illegal Content Online", *Stanford Center for Internet and Society*, 2018 (disponible en: https://ssrn.com/abstract=3262950).

KLONICK, K.: "The New Governors: The People, Rules, and Processes Governing Online Speech", *Harvard Law Review*, vol. 131, Issue 6, 2018, pp. 1599-1670.

LAPIEDRA ALCAMÍ, R.: "Restricciones impuestas por el legislador europeo a los servicios de intermediación en línea en materia de publicidad digital", CASTELLÓ PASTOR, J.J. *(Dir.), Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*), Aranzadi, 2024, pp. 205-226.

LLANSÓ, E.J., "No Amount of 'AI' In Content Moderation Will Solve Filtering's Prior Restraint Problem", *Big Data & Society,* abril 202 (https://journals.sagepub.com/doi/full/10.1177/2053951720920686).

LLANSÓ, E; VAN HOBOKEN, J.; LEERSSEN, P. Y HARAMBAM. J.: "Artificial Intelligence, Content Moderation, and Freedom of Expression", *Working paper of the Transatlantic Working Group on Content Moderation Online and Freedom of Expressio*n, 2020, p. 7 (https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf).

NAVAS NAVARRO, S "Moderación de contenido e Inteligencia artificial generativa", *Derecho y digitalización empresarial. Reflexiones sobre el impacto*

de la digitalización en el Derecho que regula la actividad empresarial. https://webs.uab.cat/derecho-y-digitalizacion-empresarial/2023/07/12/moderacion-de-contenido-e-inteligencia-artificial-generativa/

ORTEGA GIMÉNEZ, A., "La extraterritorialidad del futuro Reglamento Europeo de Inteligencia Artificial", *Revista jurídica Colex*, N.º 36, 2024, pp. 22-23.

PADÍ, A. "Así se está regulando la IA en la UE, EE.UU. y la OCDE: el difícil equilibrio entre seguridad y fomento de la innovación", 23.02.2024 (https://www.garrigues.com/es_ES/garrigues-digital/asi-esta-regulando-ia-ue-eeuu-ocde-dificil-equilibrio-seguridad-fomento).

PARISER, E., *The filter bubble: What the internet is hiding from you*, New York: Penguin Press, 2011.

VILLASCHI, P., "The Regulation of Political Targeting in the Italian and European Union Legal Framework", *Rivista di diritto internazionale privato e Processuale (RDIPP),* Gennaio-Marzo 2024, pp. 136 ss.

WILMAN, F., "The Digital Services Act (DSA): An Overview (16 de diciembre de 2022)". *Comisión Europea.* Disponible en SSRN: https://ssrn.com/abstract=4304586 (fecha consulta: 11 noviembre 2024).

View this in your browser.

Check out these new contents on the EAPIL blog EAPIL — European Association of Private International Law.

Capítulo 9

La gobernanza internacional de la Inteligencia Artificial en Naciones Unidas desde una perspectiva de Derechos Humanos*

Ana Gascón Marcén
Prof.ª Contratada Dra. de Derecho Internacional Público
Universidad de Zaragoza

SUMARIO: I. INTRODUCCIÓN. II. INICIATIVAS DE GOBERNANZA. 1. *Gobernanza interna*. 2. *Gobernanza externa*. 2.1. Informe Gobernanza de la IA en beneficio de la humanidad. 2.2. Pacto Digital Mundial. 2.3. Avances en 2025. III. ASAMBLEA GENERAL DE NACIONES UNIDAS. IV. CONSEJO DE DERECHOS HUMANOS. 1. *Marco empresa y derechos humanos*. 2. *Informes de expertos en Derechos Humanos*. V. UNESCO. VI. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. VII. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El creciente uso de la inteligencia artificial (IA) supone que aumentan las oportunidades de que su utilización afecte a nuestros derechos humanos (DDHH), desde la privacidad a la libertad de expresión e información o a la participación democrática, junto con un amplio abanico de otros derechos civiles y políticos, pero también económicos sociales o culturales, incluso el derecho al medio ambiente o nuevos derechos en debate relativos a los avances de la neurotecnología.

* Esta publicación es parte del Proyecto "Hacia una transición digital centrada en la persona en la Unión Europea" TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/PRTR, de cuyo equipo de investigación es miembro la autora. Todas las páginas web consultadas por la autora lo han sido por última vez el 31 de marzo de 2025.

Son múltiples las organizaciones internacionales que trabajan en el desarrollo de marcos normativos y gobernanza de la IA (GIA). La Organización para la Cooperación y el Desarrollo Económicos (OCDE) en su Recomendación del Consejo sobre IA de 2019 actualizada en 2024 define la IA como "un sistema basado en máquinas que, para unos objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue." Se trata de una definición hacia la que han convergido otras organizaciones internacionales como la Unión Europea o el Consejo de Europa. En esta recomendación además se establecía que los actores de la IA deben respetar el estado de derecho, los DDHH y los valores democráticos durante todo el ciclo de vida del sistema de IA, entre ellos la libertad, la dignidad y la autonomía, la privacidad y la protección de datos, la no discriminación y la igualdad, la diversidad, la equidad, la justicia social y los derechos laborales reconocidos internacionalmente.

Definir la IA es extremadamente complicado, pero también lo es definir qué es la gobernanza de ésta. El Diccionario de la Lengua de la Real Academia Española define la "gobernanza" como el "arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía." Es un término que no sólo se refiere a la regulación de una materia, sino que valiéndose de diversos instrumentos busca una serie de objetivos, en este capítulo nos centraremos en la protección de los DDHH, e integra la participación y los interese de diferentes entidades. En este caso, es un fenómeno que debe entenderse dentro del más amplio de gobernanza digital, con esfuerzos paralelos como los de la gobernanza de Internet.

VEALE *et al.* explican que una forma de entender la GIA es analizar el objetivo conceptual de la regulación. Estos autores distinguen las normas según el aspecto de la IA en la práctica que pretenden moldear.[1] La gobernanza de su desarrollo implica intentar aplicar requisitos durante el diseño y el mantenimiento del sistema para lograr una serie de objetivos de política, la del uso se refiere a los medios y fines de la implementación de *software* con consecuencias políticas, sociales y económicas, y la de las

1. VEALE, M., MATUS, K., y GORWA, R., "AI and global governance: modalities, rationales, tensions", *Annual Review of Law and Social Science,* vol. 19, núm. 1 (2023), pp. 255-275, p. 257.

infraestructuras implica iniciativas políticas que buscan trascender esta dicotomía desarrollo-uso.

En un contexto de competencia global para aprovechar las oportunidades que promete la IA, casi todos los países se han embarcado en una carrera hacia la IA. Pero, como explica SMUHA, la mayor visibilidad de los riesgos de la tecnología ha llevado a peticiones cada vez más fuertes para que los reguladores miren más allá de los beneficios y también aseguren una regulación adecuada para garantizar que la IA sea "digna de confianza", es decir, legal, ética y sólida. En consecuencia, esta autora sostiene que también se ha generado una "carrera hacia la regulación de la IA".[2] Esta competición por establecer las reglas de la IA no sólo se da entre Estados, sino también entre las organizaciones internacionales.

Antes de presentar las diferentes iniciativas hay que destacar que la GIA es muy amplia y, aunque aquí se analicen cuestiones relacionadas sobre todo con esfuerzos en el marco de organizaciones internacionales, VEALE *et al.* explican que hay otras modalidades de gobernanza con un impacto relevante como códigos éticos, gobernanza de la propia industria, contratos y licencias y estándares técnicos y, dado que el panorama global del desarrollo de la IA se caracteriza por niveles muy altos de control e influencia de la industria, la cuestión del poder privado es crucial[3].

BRYSON y BACKOVSKY critican que el terreno actual de la GIA global está profundamente fragmentado, puesto que diferentes organizaciones compiten por el dominio y la legitimidad, además de ser profundamente disfuncional.[4] El GPAI, la OCDE, la UNESCO y la Unión Internacional de Telecomunicaciones (UIT) forman un conjunto de actores que compiten entre sí y que en la actualidad no proporcionan la legitimidad y la centralización necesarias que servirían mejor a la GIA mundial. En su opinión, hace falta institucionalizar nuevas formas de gobernanza que podría extraer lecciones útiles de las que se crearon para responder a la amenaza nuclear.

Se ha elegido estudiar el ámbito universal, tomando como referencia la Organización de las Naciones Unidas (NNUU), pero no deben ignorarse en esta materia las iniciativas regionales, siendo el Reglamento de Inteligencia

2. SMUHA, N., "From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence", *Law, Innovation and Technology*, vol. 13, núm. 1 (2021), pp. 57-84.
3. VEALE *et al.*, *op. cit.*, p. 270.
4. BACKOVSKY, D. y BRYSON, J.J., "Going Nuclear? Precedents and Options for the Transnational Governance of AI", *Horizons: Journal of International Relations and Sustainable Development*, núm. 24 (2023), pp. 84-95.

Artificial de la UE, el esfuerzo más notable de regulación horizontal de la IA.[5] No obstante, también se han dado esfuerzos en otras zonas del mundo, por ejemplo, la Unión Africana aprobó una Estrategia Continental de IA en 2024. Esta estrategia subraya el compromiso de África con un enfoque de la IA centrado en el desarrollo, que promueva prácticas éticas, responsables y equitativas, guiada por los principios de ética, inclusión y diversidad, DDHH y dignidad humana, bienestar de las personas, paz y prosperidad, prioriza el desarrollo y la adaptación de los sistemas de IA al contexto de África. La Organización de Estados Americanos también ha elaborado un Marco de Referencia Interamericano de Gobernanza de Datos e IA.

Las NNUU son la organización intergubernamental universal de cooperación por excelencia que cubre un gran número de actuaciones en los ámbitos más dispares, pero que tiene entre sus propósitos principales "realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los Derechos Humanos y a las libertades fundamentales de todos"[6].

Según FOURNIER-TOMBS *et al*., muchos de los riesgos de la IA están estrechamente relacionados con los pilares de NNUU: desarrollo sostenible, DDHH, igualdad de género y paz.[7] En este sentido, un esfuerzo liderado por NNUU es crucial, no solo porque la IA requiere un foro multilateral global para su gobernanza, sino también porque una IA no regulada podría socavar otras prioridades multilaterales. Los gobiernos nacionales lideraron los primeros esfuerzos de regulación de la IA, recientemente se les han unido diversas iniciativas multilaterales y regionales, pero, según estos autores, sin NNUU para coordinar estos esfuerzos desde una perspectiva global, la GIA corre el riesgo de presentar redundancias y lagunas. La naturaleza transfronteriza de la IA, que también afecta a la gobernanza de datos, hardware e Internet, requiere el liderazgo de NNUU y la cooperación de sus 193 Estados miembros.

Según HAUSENLOY y DENNIS, el papel de NNUU en el apoyo al desarrollo de estándares y regulación para la GIA ofrece importantes ventajas, como su larga e ilustre trayectoria en la consolidación de normas globales,

5. GASCÓN MARCÉN, A., "La propuesta de Reglamento de la Comisión Europea por el que se establecen normas armonizadas en materia de inteligencia artificial", en *Retos de la sociedad digital: Regulación y fiscalidad en un contexto internacional*, Reus, 2022, pp. 11-36.
6. Art. 1.3 Carta de las Naciones Unidas.
7. FOURNIER-TOMBS, E., SIDDIQUI, M., CASTETS-RENARD, C. y NDIOR, V., *A Global Architecture for Artificial Intelligence*, United Nations University Centre for Policy Research, Technical Note, 2023.

como los DDHH, y su labor para luchar contra la desigualdad, no obstante, su composición centrada en el Estado, la falta de experiencia técnica, los retrasos burocráticos y la limitada autoridad de aplicación sobre los desarrolladores privados limitan su capacidad de supervisión regulatoria en IA[8].

Dentro de NNUU, se va a comenzar por estudiar las iniciativas puramente de gobernanza (apartado II), para luego analizar la resoluciones de la Asamblea General (AGNU) sobre IA en 2024 (apartado III), los desarrollos en el marco del Consejo de Derechos Humanos (apartado IV), la labor de otras dos organizaciones diferentes que son independientes, pero son miembros de la familia o sistema de NNUU como son UNESCO (apartado V) y la UIT (apartado VI)[9] y terminar con unas breves conclusiones (apartado VII).

II. INICIATIVAS DE GOBERNANZA

Dentro de las iniciativas de gobernanza en el marco de NNUU, vamos a diferenciar las de gobernanza interna que buscan analizar qué se está haciendo dentro de la organización para coordinar su propia acción y las de gobernanza externa centradas en ofrecer mecanismos de gobernanza para los Estados miembros y las partes interesadas.

1. GOBERNANZA INTERNA

Bajo la presidencia del Secretario General (SGNU), la Junta de los Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación (CEB por sus siglas en inglés) y sus mecanismos subsidiarios han examinado diversas cuestiones de vanguardia desde 2017 para garantizar que el sistema de NNUU esté bien posicionado para brindar apoyo y asesoramiento oportunos e informados a los Estados miembros en el actual contexto tecnológico en rápida evolución. En su sesión de 2017, la CEB comenzó a examinar los riesgos y las oportunidades para el desarrollo sostenible asociados a las tecnologías nuevas y emergentes y los avances conexos, considerando específicamente la IA, el ciberespacio y la biotecnología, así como sus implicaciones para la paz y la seguridad. El objetivo era identificar áreas apropiadas para la participación del sistema de NNUU en el ámbito de las tecnologías de

8. HAUSENLOY, J. y DENNIS, C., *Towards a UN Role in Governing Foundation Artificial Intelligence Models*, United Nations University Centre for Policy Research, Working Paper, 2023.
9. El sistema de las NNNUU está formado por la propia ONU y numerosas organizaciones afiliadas conocidas como programas, fondos y agencias especializadas. Cada uno de ellos cuenta con su propia membresía, competencias y presupuesto.

vanguardia en apoyo a los Estados miembros. Los debates se basaron en análisis elaborados por el Comité de Alto Nivel sobre Programas (HLCP). En 2019, a petición de la CEB, el HLCP finalizó su labor sobre tres temas clave de vanguardia: la IA, el futuro del trabajo y la educación innovadora, y presentó tres estrategias interrelacionadas para todo el sistema, que fueron aprobadas por la CEB. En 2020, con el fin de promover el uso responsable de la IA, la CEB aprobó los Principios para el Uso Ético de la Inteligencia Artificial en el Sistema de las Naciones Unidas.[10] Se creó un grupo de trabajo interinstitucional sobre IA (IAWG-IA) del HLCP codirigido por la UNESCO y la UIT que elaboró el Libro Blanco del Sistema de las Naciones Unidas sobre la Gobernanza de la IA,[11] tras un proceso de colaboración a nivel de todo el sistema, que analiza los modelos institucionales, las funciones y los marcos normativos internacionales existentes del sistema de NNUU aplicables a la GIA.[12] El Comité de Alto Nivel sobre Gestión (HLCM) también tiene un Grupo de sobre el uso de la IA en el sistema de NNUU que publicó en 2024 un Informe sobre el uso operativo de la IA en el sistema de las Naciones Unidas[13] con interesantes casos de uso y propuestas.

2. GOBERNANZA EXTERNA

2.1. Informe Gobernanza de la IA en beneficio de la humanidad

En su Hoja de Ruta para la Cooperación Digital (A/74/821) de 2020, el SGNU propuso la creación de un Órgano Consultivo de Alto Nivel sobre Inteligencia Artificial (HLAB por sus siglas en inglés), integrado por 39 miembros provenientes de diferentes sectores y regiones geográficas que se formó en 2023 para realizar análisis y presentar recomendaciones para la GIA internacional. El HLAB fue copresidido por la secretaria de Estado de Digitalización e Inteligencia Artificial de España, Carme Artigas. Su principal resultado tras un proceso abierto de consultas fue el *Informe Gobernanza de la IA en beneficio de la humanidad*.[14]

En este informe se destacaba, basándose en las amplias consultas realizadas tras la publicación de su informe provisional, el principio relativo a que la GIA debe basarse en la Carta de las Naciones Unidas, el derecho

10. https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system
11. https://unsceb.org/united-nations-system-white-paper-ai-governance
12. https://unsceb.org/sites/default/files/2024-04/United%20Nations%20System%20White%20Paper%20on%20AI%20Governance.pdf
13. https://unsceb.org/sites/default/files/2024-11/Report%20on%20the%20Operational%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf
14. https://www.un-ilibrary.org/content/books/9789211068009

internacional de los DDHH (DIDH) y humanitario (DIH) y otras obligaciones internacionales, que obtuvo el mayor apoyo en todos los sectores de las partes interesadas. En sus deliberaciones, el HLAB se mostró convencido de que, para mitigar los riesgos y daños de la IA, abordar los nuevos casos de uso y garantizar que la IA pueda beneficiar realmente a toda la humanidad sin dejar a nadie atrás, la GIA debe estar centrada en los DDHH y garantizar una rendición de cuentas basada en los derechos en todas las jurisdicciones. Este compromiso fundamental con los DDHH es transversal y se aplica a todas las recomendaciones formuladas en su informe final.

El HLAB puso de manifiesto una serie de lagunas en la GIA global, relativas a representación, coordinación e implementación. Partes enteras del mundo han quedado fuera de las conversaciones internacionales sobre GIA, siendo que pueden ser especialmente vulnerables a algunos de los riesgos que puede provocar. De siete iniciativas de IA destacadas que estudiaron, solo siete Estados miembros de la ONU eran parte de todas[15], mientras que 118 no eran parte de ninguna (principalmente del Sur Global). Así, por ejemplo, la citada Recomendación de la OCDE sobre IA que ha servido para definir la IA a nivel jurídico fue negociada por sus miembros que provienen fundamentalmente del Norte Global.

ADAN *et al.* denuncian que el acceso a la IA y la participación en su desarrollo y gobernanza se concentran en unos pocos países con capacidades avanzadas de IA, mientras que la "mayoría global de la IA" (definida como la población de países que abarcan principalmente África, América Latina, el sur y el sudeste de Asia y partes de Europa del Este) está en gran medida excluida.[16] Estas regiones, si bien son diversas, comparten desafíos comunes en el acceso a tecnologías avanzadas de IA e influencia sobre ellas. Este término de la "mayoría global" también ha sido utilizado por la Coalición del Foro de la Gobernanza de Internet sobre gobernanza de datos e inteligencia artificial. BELLI y GASPAR subrayan que África, Asia, América Latina y Oriente Medio son regiones a menudo subrepresentadas en los debates sobre GIA, que comparten una historia de explotación colonial y se enfrentan a dinámicas actuales de neocolonialismo digital, que se están volviendo particularmente evidentes en lo que respecta a la adopción y regulación de la IA, así como a su capacidad para contribuir a los foros mundiales de IA[17].

15. Francia, Canadá, Alemania, Italia, Japón, Reino Unido y Estados Unidos.
16. ADAN, S. N. *et al. Voice and Access in AI: Global AI Majority Participation in Artificial Intelligence Development and Governance*, Oxford Martin School of AI Governance White Paper, 2024.
17. BELLI, L. y GASPAR, W. B., "AI from the global majority: What are we debating and why?", *AI from the global majority*, FGV Direito Rio, pp. 19-28.

ADAMS argumenta que la adopción de la IA en las regiones en desarrollo también está limitada por su diseño, por ejemplo, los modelos de IA generativa se desarrollan predominantemente en inglés, lo que significa que los resultados que producen para usuarios y contextos no occidentales suelen ser inútiles, inexactos y sesgados[18]. Además, esta tecnología amenaza a la creciente clase media en los contextos en desarrollo[19].

COLOMINA y GALCERAN denuncian que, hasta ahora, el diseño, desarrollo y despliegue de la IA, así como la investigación y gobernanza de sus desafíos asociados, han sido ampliamente moldeados por el Norte Global y el mundo corporativo que marca la pauta de esta transformación. Son, mayoritariamente, la industria y las comunidades técnicas de los países occidentales las que fijan los estándares del desarrollo tecnológico; y tanto el poder político como corporativo occidental lideran el debate sobre el modelo de gobernanza digital. La visión dominante otorga a los países del Sur Global un rol más bien periférico, incluso pasivo, o de receptor de normas sobre IA. Por eso, estas autoras consideran imprescindible incorporar discursos alternativos sobre la GIA y mitigar la distribución desigual de los riesgos de los sistemas de IA, así como superar los patrones de extracción, exclusión o marginalización de un Sur Global que busca un lugar propio en la revolución digital[20].

Según el *AI Index Annual Report 2024* de Standford, hasta su publicación se habían adoptado 75 estrategias nacionales de IA. En 2023, se agregaron ocho nuevas estrategias de países de Medio Oriente, África y el Caribe, lo que demuestra la expansión mundial de formulación de políticas de IA. La lista de nuevos países que estaban desarrollando estrategias nacionales de IA en ese momento incluía: Antigua y Barbuda, Barbados, Bielorrusia, Costa Rica, Jamaica, Pakistán o Senegal. Pero una mirada al mapa mundial representativo mostraba prácticamente un vacío en África muy por detrás del resto de continentes[21].

ROBLES criticó que el estudio de la práctica mostraba que, en el marco internacional, la mayoría de las iniciativas relacionadas con la IA estaban

18. ADAMS, R., "AI Is Bad News for the Global South", *Foreign Policy*, 17/12/2014. https://foreignpolicy.com/2024/12/17/ai-global-south-inequality/
19. Hasta el 5% de los empleos están en riesgo de automatización total a partir de la IA generativa en América Latina y el Caribe y las mujeres son las más propensas a verse afectadas. GMYREK, P., WINKLER, H. y GARGANTA, S., *Buffer or Bottleneck? Employment Exposure to Generative AI and the Digital Divide in Latin America,* World Bank/ International Labour Organization, 2024.
20. COLOMINA SALÓ, C. y GALCERAN-VERCHER, M., "Las otras geopolíticas de la inteligencia artificial", *Revista CIDOB d'afers internacionals*, núm. 138 (2024), pp. 27-50.
21. STANDFORD, *AI Index Annual Report 2024*, 2024, p. 26.

localizadas en organizaciones o foros regionales o interregionales participados por países tecnológicamente desarrollados; y el ordenamiento jurídico internacional ha de activar mecanismos de respuesta de alcance universal frente a esa situación y al desafío global que implica la GIA[22], por lo que los parámetros principales para la definición de la GIA habrían de ser, en el plano institucional, la atribución a las NNUU de un liderazgo efectivo destinado, fundamentalmente, a evitar la sectorialización o la monopolización del debate por parte de los países más desarrollados y a diseñar mecanismos de coordinación o transferencia tecnológica para neutralizar, en la medida de lo posible, los efectos de esta tecnología en el crecimiento de la brecha digital entre países desarrollados y no desarrollados.

OKOLO también ha apuntado que el desarrollo y la adopción de la IA plantean desafíos únicos para estos países, especialmente en lo que respecta a la penetración de Internet, la conexión eléctrica y las preocupaciones sobre los impactos negativos de la IA[23]. En su opinión, los gobiernos del Sur Global deben invertir en investigadores locales e integrar la capacitación en habilidades digitales en los programas educativos, y los países que han dominado el debate sobre la IA deben incluir a los países del Sur Global en las mesas redondas y los órganos consultivos.

Respecto a la gobernanza, el HLAB hizo varias propuestas que suponían la creación de: un Grupo internacional de científicos expertos en IA, inspirándose en precedentes como el Grupo Intergubernamental de Expertos sobre el Cambio Climático (IPCC), que debería funcionar de forma independiente, con el apoyo de un equipo del sistema de NNUU formado por miembros de la oficina de IA que también se proponía crear, de UNESCO y la UIT[24]; un diálogo sobre políticas intergubernamental y multilateral sobre la GIA dos

22. ROBLES CARRILLO, M., "La gobernanza de la inteligencia artificial: contexto y parámetros generales", *Revista Electrónica de Estudios Internacionales,* núm. 39 (2020).

23. OKOLO, C. T., "AI in the Global South: Opportunities and challenges towards more inclusive governance", *Brookings,* 1/11/2023 *https://www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challenges-towards-more-inclusive-governance/*

24. Podría publicar un informe anual en el que se analicen las capacidades, las oportunidades, los riesgos y las incertidumbres relacionadas con la IA y se identifiquen las esferas de consenso científico sobre las tendencias tecnológicas y las áreas en las que se necesita más investigación; producir compendios trimestrales de investigación temática sobre las esferas en las que la IA podría contribuir a la consecución de los ODS, centrándose en las áreas de interés público que puedan estar insuficientemente atendidas; y publicar informes ad hoc sobre cuestiones emergentes, en particular la aparición de nuevos riesgos o las importantes lagunas existentes en el panorama de la gobernanza.

veces al año, en paralelo a las reuniones que se celebren en NNUU[25]; una entidad de intercambio de normas sobre la IA que reúna a representantes de organizaciones nacionales e internacionales de normalización, empresas tecnológicas, la sociedad civil y representantes del grupo internacional de científicos;[26] una red de desarrollo de la capacidad de IA que reúna a una serie de centros de desarrollo de capacidad afiliados a NNUU poniendo conocimientos especializados, computación y datos de entrenamiento de IA a disposición de los agentes clave; un fondo mundial de IA con el fin de reducir la brecha existente en este ámbito[27]; un marco mundial de datos sobre IA; y una oficina de IA en la Secretaría General de NNUU.

Se trata de bastantes nuevas propuestas, aunque la mayoría reciclan lo que ya se hace en otros sectores, y cabe preguntarse, por ejemplo, cuál sería la utilidad de una nueva reunión sobre IA cuando ya existen, entre otras, la reunión anual de la *AI for Good* de la UIT, la reunión anual del Foro para la Gobernanza de Internet (donde también se tratan temas de IA), el Foro sobre la Ética de la Inteligencia Artificial de la UNESCO o la *AI Safety Summit*.

ASAAD ha considerado el Informe un paso en la buena dirección, pero critica su falta de coherencia puesto que incorpora afirmaciones desequilibradas y a veces contradictorias y su falta de especificidad para su aplicación, porque en su opinión un enfoque global para la GIA solo funcionará si logra captar los matices de la especificidad de la aplicación y el dominio.[28] En la misma línea, para TIMCKE, el Informe es encomiable, pero desvía la atención de la materialidad de la IA. La base material completa (incluyendo

25. Su objetivo sería: compartir las mejores prácticas sobre GIA que respete, proteja y promueva los DDHH y fomente el desarrollo, y que incluya tanto la búsqueda de oportunidades como la gestión de riesgos; promover un entendimiento común sobre la implementación de medidas de GIA por parte de los desarrolladores y los usuarios de los sectores público y privado para mejorar la interoperabilidad internacional de la GIA; compartir voluntariamente incidentes significativos de IA que hayan sobrepasado la capacidad de respuesta de los organismos estatales; y debatir sobre los informes del Panel internacional de científicos expertos en IA.
26. Para elaborar y mantener un registro de definiciones y normas aplicables para medir y evaluar los sistemas de IA; debatir y evaluar las normas y los procesos para su elaboración; e identificar las lagunas que requieran nuevas normas.
27. Gestionado por una estructura de gobierno independiente, el fondo recibiría contribuciones financieras y en especie de fuentes públicas y privadas, y las desembolsaría, también a través de la red de desarrollo de la capacidad, para mejorar el acceso a facilitadores de la IA orientados a impulsar el empoderamiento local en pro de los ODS.
28. ASSAAD, Z., "The United Nations has a plan to govern AI — but has it bought the industry's hype?", *The Conversation*, 23/09/2024, https://theconversation.com/the-united-nations-has-a-plan-to-govern-ai-but-has-it-bought-the-industrys-hype-239494

la ubicación de los centros de datos, las leyes que los rigen y quién ostenta los derechos de control directo) abarca cuestiones importantes que difícilmente se conciliarán mediante la apelación a compromisos compartidos.[29] En su opinión, el HLAB podría haber sido más directo sobre qué áreas del desarrollo de la IA deberían desaconsejarse, siendo la decisión de excluir las cuestiones de armamento un error significativo. Para este autor, si bien el Informe avanza en el abordaje de la GIA global, algunos temas críticos parecen recibir menos énfasis, dado que las preocupaciones sobre la concentración de poder en el sector de la IA y la creciente brecha tecnológica entre países no se destacan con la misma prominencia que en el primer borrador. La posibilidad de implementar medidas redistributivas para abordar las crecientes desigualdades en el desarrollo y la implementación de la IA sigue siendo una consideración remota. El informe aborda con cautela cómo el capital está moldeando la distribución y las experiencias de las tecnologías de IA. Existe una ausencia de esfuerzos concertados para dirigir la inversión hacia el Sur Global, lo que perpetúa las jerarquías globales existentes. Los arraigados desequilibrios de poder en el desarrollo y la distribución de la IA siguen sin abordarse adecuadamente, lo que pone de relieve la necesidad de priorizar los problemas de injusticia económica en la GIA global.

2.2. Pacto Digital Mundial

En la Cumbre del Futuro de 2024, los líderes mundiales adoptaron el Pacto para el Futuro y su anexo el Pacto Digital Mundial (A/RES/79/1). Este tenía entre sus objetivos: eliminar todas las brechas digitales (incluida la de la IA) y acelerar los progresos en todos los ODS; fomentar un espacio digital inclusivo, abierto y seguro que respete, proteja y promueva los DDHH; y mejorar la GIA internacional en beneficio de la humanidad.

En concreto respecto a este último objetivo, reconocieron la necesidad de adoptar un enfoque equilibrado, inclusivo y basado en los riesgos para la GIA, con la representación plena e igualitaria de todos los países, especialmente los países en desarrollo, y la participación significativa de todos los interesados. Es urgente evaluar y abordar de forma inclusiva los posibles efectos, oportunidades y riesgos de los sistemas de inteligencia artificial para el desarrollo sostenible y el bienestar y los derechos de las personas. Se necesita cooperación internacional para promover la coordinación y la compatibilidad de los marcos de GIA que están surgiendo.

29. TIMCKE, S., "Response to the Governing AI for Humanity Report", *TechPolicy. Press*, 26/09/2024, https://www.techpolicy.press/deficits-gaps-and-compromises-in-the-uns-governing-ai-for-humanity/

Se comprometieron a: establecer, dentro de NNUU, un panel científico internacional independiente y multidisciplinar sobre la inteligencia artificial con representación geográfica equilibrada para promover el conocimiento científico mediante evaluaciones empíricas de los efectos, los riesgos y las oportunidades, aprovechando las iniciativas y las redes de investigación nacionales, regionales e internacionales existentes; iniciar, dentro de NNUU, un diálogo mundial sobre la GIA en el que intervengan los Gobiernos y todas las partes interesadas, que se celebrará paralelamente a las conferencias y reuniones pertinentes de NNUU. Así la AGNU crearía el Panel Científico Internacional Independiente sobre Inteligencia Artificial y el Diálogo Mundial sobre la Gobernanza de la Inteligencia Artificial.

Respecto al resto de propuestas del HLAB, la AGNU apoyó sus objetivos, pero no necesariamente la creación de nuevos órganos[30]. Sobre la posibilidad de crear un fondo de IA, puso de relieve la importancia de aumentar las inversiones, en particular las del sector privado y las filantrópicas, a fin de ampliar la creación de capacidad de IA para el desarrollo sostenible y solicitó al SGNU que, en consulta con los posibles contribuyentes y el sistema de NNUU, formule opciones innovadoras de financiación voluntaria para crear capacidad de IA que sirvan de complemento a los mecanismos de financiación pertinentes de las NNUU.

2.3. Avances en 2025

Si bien no se ha creado una Oficina de IA en la SGNU, a partir del 1 de enero de 2025, la Oficina del Enviado del Secretario General para la Tecnología se transformó en una nueva Oficina de las Naciones Unidas para las Tecnologías Digitales y Emergentes (ODET). Lo que se deriva de una decisión

30. La AGNU exhortó a las organizaciones normativas a que colaboren para promover la elaboración y adopción de normas interoperables de IA que propugnen la seguridad, la fiabilidad, la sostenibilidad y los derechos humanos; alentó el establecimiento de alianzas internacionales para crear capacidad de IA con el fin de elaborar programas de educación y formación, aumentar el acceso a los recursos, incluidos los modelos y sistemas de IA abiertos, los datos abiertos de entrenamiento y computación abierta, facilitar el entrenamiento y desarrollo de modelos de IA y promover la participación de las microempresas y pequeñas y medianas empresas en la economía digital; decidió aprovechar los mecanismos existentes de las NNUU y de múltiples partes interesadas para apoyar la creación de capacidad en IA con el fin de reducir las disparidades en ese ámbito, facilitar el acceso a las aplicaciones de IA y aumentar la capacidad de computación de alto rendimiento y destrezas afines en los países en y promover la cooperación Norte-Sur, Sur-Sur y triangular para apoyar el desarrollo de conjuntos de datos representativos de alta calidad, recursos informáticos asequibles, soluciones locales que reflejen la diversidad lingüística y cultural y ecosistemas empresariales en los países en desarrollo.

de la AGNU para darle un mandato reforzado. La ODET actuará para: servir como promotor y punto focal de la cooperación digital en NNUU para los Estados miembros y las partes interesadas; facilitar un diálogo inclusivo y de múltiples partes interesadas sobre políticas relativas a las tecnologías digitales y emergentes; asesorar a los altos directivos de NNUU sobre las tendencias tecnológicas clave a fin de orientar el enfoque estratégico adoptado por la organización sobre esas cuestiones; fortalecer la coordinación a nivel de todo el sistema de NNUU sobre las tecnologías digitales y emergentes; y apoyar el seguimiento y la aplicación del Pacto Digital Mundial, incluyendo la GIA[31].

En noviembre de 2024, el Presidente de la AGNU nombró a los Representantes Permanentes de España y Costa Rica ante NNUU como cofacilitadores para liderar el proceso intergubernamental para definir los términos de referencia y las modalidades de funcionamiento del Panel Científico Independiente Internacional y del Diálogo Global sobre Gobernanza de la Inteligencia Artificial. Estos llevaron a cabo una serie de consultas y presentaron en marzo de 2025 un primer borrador que se someterá a posteriores revisiones para su aprobación última por la AGNU en 2025.

En el borrador se propone que el Panel Científico Internacional Independiente sobre Inteligencia Artificial esté formado por un Comité de Expertos integrado por veinte miembros designados por el SGNU, que ejercerán sus funciones a título personal y serán seleccionados por su experiencia en la esfera de la IA y campos conexos, por un período de tres años, renovable una vez; y un Comité Asesor integrado por cuarenta miembros elegidos por la AGNU, que ejercerán sus funciones a título personal y serán seleccionados por su experiencia en la esfera de la IA y campos conexos, por un período de tres años, renovable una vez. Al elegir a los miembros del Comité Asesor, la AGNU distribuirá los cuarenta puestos equitativamente entre los grupos regionales, teniendo debidamente en cuenta la experiencia destacada de los candidatos, la representación multidisciplinaria diversa y el equilibrio geográfico y de género. Además, el Comité de Expertos estará presidido por dos de sus miembros, uno de un país en desarrollo y otro de un país desarrollado, designados por el SGNU. El Grupo elaborará, entre otros, un informe anual que sintetice las tendencias clave de investigación en IA.

Por su parte, el Diálogo Global sobre la Gobernanza de la Inteligencia Artificial será una plataforma intergubernamental y de múltiples partes interesadas para facilitar debates abiertos, transparentes e inclusivos sobre

31. https://www.un.org/digital-emerging-technologies/content/press-release-new-un-office-digital-and-emerging-technologies A/RES/79/258

la GIA, fomentando al mismo tiempo las sinergias con todas las iniciativas existentes sobre IA en NNUU. El Grupo de Expertos presentará sus conclusiones al Diálogo. El Diálogo facilitará la cooperación internacional en GIA mediante el intercambio de mejores prácticas, lecciones aprendidas y programas de desarrollo de capacidades; identificará maneras en que la IA puede contribuir a la implementación de los ODS, el respeto, la protección y la promoción de los DDHH, apoyará la diversidad lingüística y cultural; fomentará el diálogo entre los Estados miembros y las partes interesadas; y la interoperabilidad. El Diálogo estará abierto a todos los Estados miembros, observadores y partes interesadas pertinentes; y celebrará una sesión plenaria, con un segmento de alto nivel con participación de Jefes de Estado y de Gobierno, y debates temáticos. Se convocará una vez al año en paralelo a las conferencias y reuniones pertinentes de NNUU. El Presidente de la AGNU designará dos copresidentes para cada reunión anual, uno de un país en desarrollo y otro de un país desarrollado, quienes identificarán los temas del Diálogo y prepararán un resumen del mismo. El primer Diálogo tendrá lugar en Nueva York en septiembre de 2025.

El SGNU pondrá en funcionamiento una Secretaría para brindar el apoyo necesario al Grupo de Expertos y al Diálogo, aprovechando las capacidades de todo el sistema, incluidas las de la ODET, la UIT y UNESCO.

III. ASAMBLEA GENERAL DE NACIONES UNIDAS

Hemos de tener presente que textos como la Declaración Universal de Derechos Humanos (DUDH) aprobada a través de una resolución de la AGNU en 1948, como todos los tratados internacionales de protección de DDHH adoptados en el marco de NNUU son aplicables también al uso y desarrollo de la IA. De manera más específica, desde 2013, la AGNU y el Consejo de Derechos Humanos (CDH) han aprobado numerosas resoluciones sobre el derecho a la privacidad en la era digital.

En 2023, la AGNU adoptó una Resolución sobre la promoción y protección de los derechos humanos en el contexto de las tecnologías digitales (A/RES/78/213) centrada en la IA, si bien el título de la misma era más amplio y tocaba otras cuestiones como la identidad digital, por ejemplo. En ella observó que el uso de la IA podía contribuir a promover y proteger los DDHH y llegar a transformar los Gobiernos y las sociedades, los sectores económicos y el mundo del trabajo, pero también explicitó su preocupación por que ésta o las tecnologías de aprendizaje automático puedan, sin las debidas salvaguardias de DDHH y técnicas, reglamentarias, jurídicas y éticas, y sin mecanismos

adecuados y eficaces de evaluación y recopilación de observaciones, conllevar el riesgo de reforzar la discriminación sistémica, racial y por razón de género y dar lugar a decisiones que podrían afectar al disfrute de los DDHH, incluidos los derechos económicos, sociales y culturales, y menoscabar la no discriminación, y reconociendo la necesidad de prevenir resultados discriminatorios por cuestiones de raza y de otro tipo y aplicar el DIDH y marcos de protección de datos en la concepción, el diseño, el desarrollo, el despliegue, el uso, la evaluación y la regulación de esas tecnologías y prácticas. La AGNU afirmó que se deben respetar, proteger y promover los DDHH y las libertades fundamentales durante todo el ciclo vital de los sistemas de IA y que las tecnologías digitales nuevas y emergentes deberían proporcionar nuevas formas de promover, proteger y ejercer los DDHH, y no menoscabarlos. Exhortó a los Estados y a las partes interesadas, a que: apliquen la diligencia debida de DDHH, lo que incluye evaluaciones periódicas y exhaustivas del impacto en los mismos de la IA, durante todo su ciclo vital, a fin de prevenir y mitigar sus repercusiones negativas en los DDHH y garantizar recursos efectivos y la vigilancia humana, la rendición de cuentas y la responsabilidad jurídica; prevengan el daño a las personas causado por los sistemas de IA y se abstengan o dejen de usar aplicaciones de IA que son imposibles de operar en consonancia con el DIDH o que suponen riesgos indebidos para el disfrute de los DDHH, a menos y hasta que existan las salvaguardias adecuadas para proteger los DDHH y las libertades fundamentales; promuevan la transparencia de los sistemas de IA y la explicabilidad adecuada de las decisiones basadas en la IA, teniendo en consideración los distintos riesgos para los DDHH derivados de esas tecnologías; y alentó a los Estados y las empresas a velar por que participen todas las partes interesadas pertinentes en las decisiones sobre el desarrollo, el despliegue y el uso de la IA.

Finalmente, en marzo de 2024, la AGNU adoptó por aclamación (es decir sin voto) una resolución específica sobre la IA, más en particular para aprovechar las oportunidades de sistemas seguros y fiables de IA para el desarrollo sostenible (A/RES/78/265). El proyecto de resolución fue liderado por Estados Unidos[32], copatrocinado o respaldado por más de 125 Estados. La resolución empieza reafirmando el compromiso con el derecho

32. Hay que tener en cuenta que se trataba todavía de la Administración Biden que sin tener un enfoque marcadamente regulatorio sí que era partidario de crear ciertas salvaguardias respecto al desarrollo de la IA, lo que ha cambiado con la Administración Trump que es partidario de una fuerte desregulación en este ámbito, véase GASCÓN MARCÉN, A., "La gobernanza de la inteligencia artificial en Estados Unidos y China, modelos regulatorios alternativos al europeo", en *Actualidad legislativa y jurisprudencial: el Derecho ante el reto de las tecnologías disruptivas*, Colex, 2025.

internacional y recordando específicamente la DUDH. Esto es un signo de que se intenta que éstos sean pilar fundamental de la misma y las menciones a los DDHH se repiten a lo largo de todo el documento.

La AGNU reconoció que unos sistemas seguros y fiables de IA —cuyo ciclo de vida incluye las etapas de prediseño, diseño, desarrollo, evaluación, puesta a prueba, despliegue, utilización, venta, adquisición, explotación y retirada de servicio, y presentan las siguientes características: están centrados en las personas, son fiables, se pueden explicar, son éticos e inclusivos, respetan plenamente la promoción y la protección de los DDHH y el derecho internacional, mantienen la privacidad, están orientados al desarrollo sostenible y son responsables— tienen el potencial de acelerar y propiciar los avances hacia la consecución de los 17 Objetivos de Desarrollo Sostenible (ODS) y el desarrollo sostenible en sus tres dimensiones —económica, social y ambiental— de manera equilibrada e integrada, fomentar la transformación digital, promover la paz, salvar las brechas digitales entre los países y dentro de ellos y promover y proteger el goce de los DDHH y las libertades fundamentales para todos, manteniendo a la persona en el centro. Esta frase sacada de la resolución deja vislumbrar que se intentaron incluir muchos elementos para contentar a todas las partes. No obstante, también hay elementos que se dejaron fuera para lograr el consenso como los sistemas de IA en el ámbito militar.

RODRÍGUEZ explica que los intereses estatales en este ámbito y la especialidad de las materias que se aglutinan en el campo militar apuntan claramente a que los progresos regulatorios que puedan alcanzarse estarán sectorializados y esto induce a intuir que los avances generales que se produzcan en una posible regulación general de la IA no van a suscitar consensos que se extiendan al ámbito de la defensa, que parece reservado a dominios especializados.[33] El autor pone como ejemplo específico esta resolución al destacar que, incluso en el marco de la AGNU, la primera aproximación a la IA pidiendo una regulación internacional y una especial cooperación para evitar que estas tecnologías funcionen de forma acorde con los DDHH se ha excluido expresamente su aplicación al ámbito militar.

La AGNU reconoció también que el diseño, el desarrollo y la utilización incorrectos o maliciosos de los sistemas de IA, por ejemplo, sin salvaguardias adecuadas o de manera contraria al derecho internacional, plantea riesgos que podrían dificultar los avances hacia la consecución de la Agenda 2030 y sus ODS y socavar el desarrollo sostenible en sus tres dimensiones, agrandar las brechas digitales entre los países y dentro de ellos, reforzar las desigualdades

33. RODRÍGUEZ, J. M., "La regulación de la inteligencia artificial y la responsabilidad de los Estados en su utilización militar", *Revista UNISCI*, núm. 67 (2025), pp. 53-86.

y los sesgos estructurales, conducir a la discriminación, minar la integridad de la información y el acceso a ella, debilitar la protección, la promoción y el goce de los DDHH y las libertades fundamentales, incluido el derecho a no sufrir injerencia ilícita o arbitraria en la vida privada, y aumentar el riesgo potencial de accidentes y amenazas complejas de actores malintencionados.

La AGNU destacó que se deben respetar, proteger y promover los DDHH y las libertades fundamentales durante todo el ciclo de vida de los sistemas de IA, exhortó a todos los Estados y a otros interesados a que se abstengan o dejen de usar sistemas de IA que sean imposibles de operar en consonancia con el derecho internacional o que supongan riesgos indebidos para el disfrute de los DDHH, en especial de quienes se encuentran en situaciones vulnerables, y reafirma que los derechos de las personas también deben estar protegidos en Internet, también durante el ciclo de vida de los sistemas de IA.

La AGNU alentó a todos los Estados miembros a que, en consonancia con sus prioridades y circunstancias nacionales y al tiempo que aplican sus distintos enfoques y marcos regulatorios y de gobernanza nacionales, y, en su caso, a otros interesados, promuevan sistemas seguros y fiables de IA de manera inclusiva y equitativa y para el beneficio de todos, y a que fomenten un entorno propicio para esos sistemas a fin de hacer frente a los mayores retos del mundo, fortaleciendo la inversión en la elaboración y la aplicación de salvaguardias eficaces, incluidas evaluaciones de riesgos y del impacto, a lo largo de todo el ciclo de vida de los sistemas de IA para proteger el goce pleno y efectivo de los DDHH y las libertades fundamentales y mitigar el posible impacto en él. Desgraciadamente, a pesar de que esta fue una resolución liderada por Estados Unidos, el Presidente Trump el primer día de su segundo mandato adoptó una orden ejecutiva que derogaba la anterior Orden ejecutiva del Presidente Biden que había puesto las pocas salvaguardas existentes en este país a nivel federal.

Para KNAUER, esta resolución presenta algunas conclusiones prometedoras, comprometiendo a los Estados a garantizar el manejo seguro de la tecnología, de conformidad con las obligaciones de DDHH, no obstante la necesidad de buscar consenso hizo que ésta fuera relativamente limitada, aun así, la resolución parece más concreta y con una redacción más contundente de lo que cabría esperar.[34] En particular, la referencia al DIDH es importante para los Estados que promueven un uso ético y seguro de la IA en sus estrategias nacionales. Además, dos nociones destacan especialmente

34. KNAUER, A., "The First United Nations General Assembly Resolution on Artificial Intelligence", *EJIL:Talk!,* 2/04/2024 https://www.ejiltalk.org/the-first-united-nations-general-assembly-resolution-on-artificial-intelligence/

en la resolución y presumiblemente contribuyeron a su éxito. La primera es una referencia recurrente al ciclo de vida de la IA, y, en segundo lugar, el texto de la resolución reafirma repetidamente que los Estados solo deben cumplir sus funciones de conformidad con el derecho nacional, garantizando un amplio margen de discreción para los Estados en lo que respecta a la implementación. Comparar la resolución con un borrador anterior de 2023 ofrece información adicional. Si bien el borrador condenaba cualquier uso indebido de la IA, la resolución final solo alienta a los Estados miembros a facilitar el desarrollo de marcos para proteger a las personas del uso indebido, entre otras prácticas nocivas. Además, inicialmente se instó a los Estados miembros a participar en varias acciones específicas relativas a la GIA. El documento final redujo esto a un simple estímulo para que los Estados actuaran. En su última sección, el borrador incluso decidió mantener los avances en el ámbito de la GIA bajo consideración para los procesos pertinentes de la ONU. La resolución final concluye con un simple reconocimiento del papel de la ONU en el logro de un consenso global sobre sistemas de IA seguros y fiables. Estos cambios muestran una flexibilización en la redacción de la resolución en comparación con el borrador anterior, lo que posiblemente facilitó significativamente su aceptación. Sin embargo, en un aspecto, la resolución final es, de hecho, considerablemente más contundente que el borrador. En cuanto a la inclusión de los países en desarrollo, el borrador inicialmente solo alentaba a los países desarrollados a ayudar a otros Estados a cerrar la brecha digital. En cambio, la resolución final insta a todos los Estados a cooperar con los países en desarrollo y brindarles asistencia, haciendo hincapié en el acceso inclusivo y equitativo a los beneficios de la IA e incluso mencionando medidas específicas que deberían adoptarse.

En julio de ese mismo año, la AGNU adoptó otra resolución especialmente dedicada a aumentar la cooperación internacional para la creación de capacidad en IA liderada por China y copatrocinada por otros 140 Estados entre los que se encontraban los Estados Unidos adoptada también por aclamación (A/RES/78/311).

Esta resolución contenía algunas menciones a los DDHH, aunque menos, porque se centraba en luchar contra la brecha existente en el marco de la IA y cómo mejorar la cooperación y financiación para que los países menos desarrollados también puedan aprovechar las oportunidades que brinda. China buscaba así posicionarse como líder y defensora de los países del Sur Global rezagados en esta materia[35].

35. Véase GASCÓN MARCÉN, A., "El Sur Global y la pugna por la regulación digital internacional", (pendiente de publicación 2025).

Es importante destacar que, si bien las resoluciones de la AGNU no son jurídicamente vinculantes, como explica FAJARDO el *soft law* refleja una intensidad normativa acorde con el consenso imperfecto que se alcanza en tiempos de crisis normativa, cuando no hay apetito por los tratados y por los procesos de formación de normas consuetudinarias que se ven contestados más que nunca por objeciones a la universalidad de las propuestas.[36] El *soft law*, en palabras de esta autora, rompe las costuras de la categoría de fuentes y ofrece una fórmula de "legalización" de los nuevos sectores normativos (como puede ser el de la IA) del Derecho Internacional con un coste político y jurídico menor que los instrumentos tradicionales. FAJARDO cita particularmente la posición de la Corte Internacional de Justicia sobre las resoluciones de la AGNU que, a través de la evolución de su jurisprudencia, ha acabado reconociendo el valor normativo, aunque no vinculante, del *soft law* internacional y más cuando se trata de resoluciones como las explicadas adoptadas por aclamación sin ningún voto en contra y con un número tan elevado de copatrocinadores.

Estas cuestiones son tremendamente relevantes porque la mayoría de las iniciativas internacionales de GIA se realizan a través de *soft law*, con excepción del Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho[37].

La última Resolución de la AGNU sobre la IA en 2024 fue la que trató sobre la IA en el ámbito militar y sus implicaciones para la paz y la seguridad internacionales (A/RES/79/239), coliderada por Corea del Sur y Países Bajos. Ésta a diferencia de las anteriores sí se sometió a voto, obteniendo 159 votos a favor entre los que se encontraban China o EEU, pero también 2 en contra de Rusia y Corea del Norte. Como elemento destacable ésta empieza afirmando que el derecho internacional, incluidos la Carta de las Naciones Unidas, el DIH y el DIDH, se aplica a las cuestiones que por él se rigen y que surgen a lo largo del ciclo de vida de las capacidades de IA, así como de los sistemas que habilitan esas capacidades en el ámbito militar. Esto debería ser evidente, no obstante, como hemos visto el ámbito militar se dejó fuera de las anteriores resoluciones. Más allá de ello no se vuelven a nombrar los DDHH y no se crean compromisos muy exigentes, si bien como continuación al trabajo realizado se solicitó al SGNU que recabe las opiniones de los Estados sobre las oportunidades y los retos que plantea

36. FAJARDO DEL CASTILLO, T., *El soft law en el Derecho Internacional y Europeo: Su capacidad para dar respuesta a los desafíos normativos actuales*, Tirant Lo Blanch, 2024.

37. Véase GASCÓN MARCÉN, A., "Nuevo Convenio Marco sobre Inteligencia Artificial del Consejo de Europa", *Derecho Digital e Innovación. Digital Law and Innovation Review,* núm. 20 (2024).

para la paz y la seguridad internacionales la aplicación de la IA en el ámbito militar, con atención específica a los ámbitos distintos de los sistemas de armas autónomos letales, y que, en su octogésimo período de sesiones, le presente un informe sustantivo en el que se resuman esas opiniones y se clasifiquen las propuestas normativas existentes y emergentes, con un anexo en el que figuren esas opiniones, para que los Estados sigan debatiendo. El SGNU también debía recabar las opiniones de las organizaciones internacionales y regionales, el Comité Internacional de la Cruz Roja, la sociedad civil, la comunidad científica y el sector industrial.

En realidad, paralelamente NNUU ya trabajaba en este tema a través del Grupo de Expertos Gubernamentales sobre las Tecnologías Emergentes en el Ámbito de los Sistemas de Armas Autónomos Letales, establecido en virtud de la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales. Hace más de diez años que existe una campaña internacional para detener los robots asesinos (*Stop Killer Robots*) a través de una coalición internacional de organizaciones no gubernamentales que exige la prohibición preventiva de la robótica autónoma letal[38]. La campaña insta a todos los Estados a: establecer una moratoria nacional sobre la robótica autónoma letal; declarar, unilateralmente y a través de foros multilaterales, el compromiso de respetar el DIH y el DIDH en todas las actividades relacionadas con las armas robóticas, e implementar procesos rigurosos para garantizar su cumplimiento en todas las etapas de desarrollo; comprometerse a ser lo más transparente posible en los procesos internos de revisión de armas; y participar en el debate internacional y el diálogo intergubernamental sobre la cuestión y estar dispuestos a intercambiar buenas prácticas con otros Estados.

Desde 2018, el SGNU ha mantenido que los sistemas de armas autónomas letales son políticamente inaceptables y moralmente repugnantes, y ha instado a prohibirlos en virtud del derecho internacional. En su Nueva Agenda para la Paz de 2023, el SGNU reiteró este llamamiento y recomendó a los Estados que, para 2026, concluyeran un instrumento jurídicamente vinculante para prohibir los sistemas de armas autónomas letales que funcionan sin control ni supervisión humana y que no pueden utilizarse de conformidad con el DIH, y para regular todos los demás tipos de sistemas de armas autónomas. Señaló que, en ausencia de regulaciones multilaterales específicas, el diseño, el desarrollo y el uso de estos sistemas plantean preocupaciones humanitarias, jurídicas, de seguridad y éticas, y representan una amenaza directa para los DDHH y las libertades fundamentales[39].

38. https://www.stopkillerrobots.org/
39. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/

La resolución reconoce las oportunidades y beneficios potenciales de la IA en el ámbito militar, como por ejemplo en las áreas de cumplimiento del DIH, incluida la protección de los civiles y los bienes de carácter civil en los conflictos armados. Sin embargo, LAHMANN ha criticado que, a través de esta invocación ritual de las mejoras esperadas en precisión y exactitud, las normas de selección de objetivos del DIH han llegado a funcionar como un marco retórico justificativo para el continuo afianzamiento de prácticas de vigilancia integrales en zonas de conflicto.[40] Porque, independientemente de si las afirmaciones sobre una mayor adhesión al DIH y la protección de la vida de los civiles se sustentarán alguna vez ante un escrutinio riguroso, estas afirmaciones optimistas no tienen en cuenta cuántos de los sistemas de seguridad de IA que se utilizan actualmente funcionan realmente. Esto constituye un problema, ya que desvía la atención de los costos sociales más amplios derivados del despliegue de dichos sistemas. El uso de IA en el ámbito militar ha tenido un efecto devastador en los DDHH como se está viendo en el conflicto en Gaza[41] y ha sido denunciado por los expertos de la ONU[42].

IV. CONSEJO DE DERECHOS HUMANOS

Dentro de este apartado vamos a comenzar describiendo el trabajo en el sector que parece más apropiado para la GIA desde una perspectiva de DDHH, que es el marco empresa y DDHH (apartado 1) que busca mejorar la aplicación de los DDHH por las empresas, pero también los informes de relatores especiales de DDHH sobre el impacto de la IA en sus ámbitos de trabajo y el balance del Alto Comisionado para DDHH de las NNUU (apartado 2), todos los cuales caen bajo la supervisión del CDH.

---

40. LAHMANN, H., "Gaza and the Collective Political Costs of Algorithmic Warfare", *EJIL:Talk!,* 25/03/2025 https://www.ejiltalk.org/gaza-and-the-collective-political-costs-of-algorithmic-warfare/
41. FATAFTA, M. y LEUFEUR, D., "Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes", *Access Now*, 9/05/2024 https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/
42. Gaza: UN experts deplore use of purported AI to commit "domicide" in Gaza, call for reparative approach to rebuilding, https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call#:~:text=GENEVA%20%2815%20April%202024%29%20%E2%80%93%20UN%20experts%20today,the%20civilian%20population%2C%20housing%2C%20vital%20services%20and%20infrastructure.

1. MARCO EMPRESA Y DERECHOS HUMANOS

Para estudiar cómo hacer frente al gran impacto en el disfrute de los DDHH que pueden tener las actividades de las empresas en general, se nombró al Representante Especial de la Organización de las Naciones Unidas, John Ruggie que propuso los Principios Rectores sobre Empresas y Derechos Humanos, respaldados por el CDH en junio de 2011. Estos Principios constituyen un conjunto de pautas para que los Estados y las empresas eviten, aborden y remedien los abusos contra los DDHH cometidos en las operaciones comerciales. Estos Principios reconocen que los Estados son los principales sujetos obligados a respetar, proteger y cumplir los estándares de DDHH y las libertades fundamentales, lo que significa no sólo que no deben infringirlos, sino también que deben crear un marco legal donde las empresas tampoco puedan hacerlo. El papel de las empresas como órganos de la sociedad que realizan funciones especializadas les exige cumplir con todas las leyes aplicables y respetar los DDHH. Finalmente, los Principios subrayan la necesidad de que los derechos y las obligaciones se correspondan con los recursos apropiados y efectivos cuando las empresas los violan.

Como se señala en el objetivo 1.3 de la Hoja de ruta para el próximo decenio sobre empresas y derechos humanos (Hoja de ruta de los Principios Rectores 10+), los Principios Rectores proporcionan un punto de partida convincente para las empresas y los Estados que tratan de enfrentar los posibles daños de las tecnologías digitales gestionando eficazmente los riesgos asociados para las personas, cuando tratan de colmar la brecha entre el rápido cambio y la capacidad de la sociedad para gestionar sus consecuencias.

El Alto Comisionado de NNUU para los DDHH (ACNUDH) presentó en 2022 un Informe sobre *La aplicación práctica de los Principios Rectores sobre las Empresas y los Derechos Humanos a las actividades de las empresas tecnológicas*[43]. En este Informe reconoció que está bien documentado que las nuevas tecnologías digitales, como la IA pueden contribuir a lograr efectos sociales, económicos y de desarrollo positivos, y que los adelantos generales de las tecnologías digitales contribuyen al logro de los ODS. Sin embargo, el uso de estas mismas tecnologías por parte de las empresas, los organismos públicos, los consumidores y el público en general también puede tener efectos negativos en la vida de las personas, a veces de forma grave e irreparable, por ejemplo, la "discriminación algorítmica" puede menoscabar la capacidad de las personas para disfrutar de sus DDHH y el uso de IA por las fuerzas del orden y el sistema de justicia penal podría tener un impacto en el derecho de una persona a no ser detenida arbitrariamente o a la igualdad ante la ley. En

43. A/HRC/50/56.

relación con el desarrollo y el uso de tecnologías digitales, como las que se basan en la IA, muchos Estados están elaborando marcos de política a nivel nacional y multilateral, sobre todo en relación con la protección de datos. Estos avances, en particular las propuestas relacionadas con los requisitos de diligencia debida de DDHH de obligado cumplimiento para las empresas[44], tendrán implicaciones en la forma en que las empresas tecnológicas diseñan, desarrollan y venden productos y servicios, por ejemplo, cuando se les exige una mayor transparencia sobre los efectos de sus actividades en los DDHH y las medidas de mitigación aplicadas.

Entre las recomendaciones de este informe relativas a la diligencia debida podemos destacar que se instaba: a los Estados a adoptar medidas adecuadas que obliguen a las empresas tecnológicas a actuar con la debida diligencia en DDHH; a las empresas de tecnología digital a respetar los DDHH, ejercer una sólida diligencia debida de DDHH en todas sus actividades y relaciones comerciales a fin de determinar, prevenir y mitigar las consecuencias negativas efectivas y potenciales sobre los DDHH y rendir cuentas de cómo las enfrentan, entre otras cosas, en relación con los riesgos para los derechos humanos derivados de sus modelos de negocio y mejorar la colaboración con los expertos y las partes interesadas afectadas, en todos los aspectos de la diligencia debida de DDHH, en particular en el Sur Global; y a los inversores a asumir plenamente su responsabilidad de integrar las consideraciones de derechos humanos en todas las etapas de la inversión, utilizar su influencia para incentivar a las empresas tecnológicas a ejercer una diligencia debida realmente útil de DDHH e influir en las opciones de modelos de negocio de las empresas en las que invierten.

En junio de 2025, el Grupo de Trabajo sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales presentará al CDH un informe sobre el uso de la IA y los Principios Rectores sobre empresas y DDHH. El informe pretende aclarar el deber y la responsabilidad respectivos de los Estados y las empresas ajenas al sector tecnológico entendido aquí como empresas que no desarrollan IA, de proteger y respetar los DDHH, así como el papel de otras partes interesadas, como la sociedad civil, las personas defensoras de DDHH, el mundo académico y las organizaciones sindicales, en el contexto de la evolución del panorama de la contratación y el despliegue de la IA.

---

44. Véase GASCÓN MARCÉN, A., "La diligencia debida en los Reglamentos de Servicios Digitales e Inteligencia Artificial", *Empresa y derechos humanos: retos y tendencias normativas ante un complejo e inédito contexto geoestratégico*, Aranzadi La Ley, 2025, pp. 231-250.

2. INFORMES DE EXPERTOS EN DERECHOS HUMANOS

El primer Informe de un relator especial centrado en analizar el impacto de la IA en los DDHH fue el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre las consecuencias de IA en el entorno de la información de 2018 (A/73/348). En él, se analizan las características especiales que hacen que la IA presente problemas específicos como son: la automatización de la toma de decisiones, la gran capacidad de análisis de datos que tiene y su adaptabilidad.[45] El Relator apostó por un enfoque de la IA basado en los DDHH no sólo por parte de los Estados sino también de las empresas. Para concretizar los Principios Rectores sobre las Empresas y los DDHH de NNUU en este campo es necesario que las empresas asuman compromisos orientados a respetar los DDHH de sus usuarios en todas las aplicaciones de IA; se abstengan de causar o contribuir a cualquier efecto negativo para los DDHH de la IA y prevenir o mitigar todo efecto negativo relacionado con sus operaciones; hagan operaciones de diligencia debida sobre los sistemas de IA para determinar y resolver las posibles repercusiones en los derechos DDHH; apliquen estrategias de prevención y mitigación; hagan un seguimiento continuo de las actividades relacionadas con la IA, en particular mediante consultas con los interesados y consultas públicas; y ofrezcan mecanismos de reclamación accesibles para remediar los efectos negativos en los DDHH de los sistemas de IA. El Relator consideró que proponer una ley o regulación integral de la IA podía ser inadecuado para un campo tan innovador, dado que tendría que ser muy general y podría terminar siendo demasiado vaga o demasiado restrictiva. En ese sentido, la regulación sectorial puede ser preferible, si bien, los Estados deben garantizar que la IA se desarrolle de conformidad con las normas de DDHH. Cualquier esfuerzo por desarrollar una política o regulación estatal en el campo de la IA debe garantizar este tipo de consideraciones. El Relator propuso medidas concretas para cumplir con los

45. Como afirma CASTELLÓ, en los últimos años, el uso de la IA para la moderación de contenidos se ha convertido en una práctica habitual entre las grandes plataformas en línea y buscadores y estos sofisticados sistemas algorítmicos desempeñan funciones esenciales al detectar, restringir y eliminar con celeridad contenidos considerados ilícitos (o incompatibles con las condiciones generales) en la red. Esta creciente utilización de la IA responde al exponencial incremento del volumen de datos y al ritmo acelerado de creación y difusión de contenidos en internet. Sin embargo, este autor avisa de que su aplicación requiere ser tratada con cautela porque puede conducir a resultados equívocos con el consiguiente impacto negativo en los derechos y libertades constitucionalmente protegidos de los usuarios digitales. CASTELLÓ PASTOR, J. J., "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea". *Cuadernos de Derecho Transnacional*, vol. 17, núm. 1 (2025), pp. 308-328.

principios expuestos como son: las evaluaciones de impacto de la IA sobre los DDHH; las auditorías externas que presentan problemas al enfrentarse a algoritmos protegidos pero que podrían elaborarse incluso sin acceso directo al código o permitiéndoselo sólo a algunos terceros certificados; y los mecanismos de refuerzo de la autonomía individual. El Relator también planteó dar publicidad al uso de la IA a través de obligaciones de información y notificación, ya que a través del uso del lenguaje natural una persona puede llegar a ignorar completamente que está interactuando con una máquina.

En 2019 el Relator sobre la extrema pobreza y los DDHH realizó un informe sobre el estado de bienestar digital (A/74/493). En él ponía de manifiesto cómo se había estudiado bastante el efecto de la IA sobre los derechos civiles y políticos, pero mucho menos sobre los sociales. Sin embargo, los sistemas de asistencia y protección social se basan cada vez más en datos y tecnologías digitales que se utilizan para automatizar, predecir, identificar, vigilar, detectar, singularizar y castigar. En el Informe se reconocía el irresistible atractivo que lleva a los Gobiernos a avanzar en esa dirección, pero se destacaba el grave riesgo de desembocar, sin ser conscientes de ello, en una distopía de bienestar digital. Se argüía que las grandes empresas tecnológicas actúan en una esfera en la que los DDHH están prácticamente ausentes, lo que es problemático sobre todo porque el sector privado está asumiendo un papel cada vez más importante en el diseño, la construcción e incluso el funcionamiento de partes importantes del estado de bienestar digital. En el Informe se recomendaba que, en lugar de obsesionarse con el fraude, el ahorro, las sanciones y las definiciones de eficiencia determinadas por el mercado, el punto de partida sea cómo transformar los presupuestos de asistencia social mediante la tecnología para mejorar el nivel de vida de las personas vulnerables y desfavorecidas.

En 2024, la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia presentó un Informe en el que abordó las formas en que la suposición predominante de que la tecnología es objetiva y neutra está propiciando que la IA perpetúe la discriminación racial (A/HRC/56/68). La Relatora examinó cuatro formas transversales en las que puede contribuir a las manifestaciones de discriminación racial: los problemas relacionados con los datos, las cuestiones de diseño de algoritmos, el uso intencionadamente discriminatorio de la IA y las cuestiones relativas a la rendición de cuentas. En especial le preocupaba su uso con efectos discriminatorios en: la aplicación de la ley, seguridad y sistema de justicia penal (identificación automática, policía predictiva, evaluación de reincidencia y sistemas de armas autóno-

mos), atención de la salud (puntuaciones de riesgo sanitario, detección de enfermedades y dispositivos médicos con IA), y educación (algoritmos de éxito académico y profesional, algoritmos de calificación, grandes modelos lingüísticos y educación y reconocimiento facial en centros educativos).

Esta es sólo una muestra de los múltiples ámbitos de DDHH tocados por la IA. En 2024 el ACNUDH publicó un *Informe de exposición: los derechos humanos y las tecnologías digitales nuevas y emergentes*, incluida la IA (A/HRC/56/45), en el que ofrecía una recopilación de la labor y las recomendaciones en la materia del CDH, su propia Oficina, los órganos de tratados de DDHH y los procedimientos especiales. En el informe se exponen las lagunas y los desafíos y se formulan recomendaciones sobre cómo abordarlos, teniendo debidamente en cuenta la labor conexa de todo el sistema de NNUU.

Destacó más allá de los informes comentados que los titulares de mandatos de los procedimientos especiales han examinado la IA y los DDHH, en informes sobre las consecuencias de la IA en los derechos a la privacidad, a la libertad de pensamiento, a la educación y a la salud, en los derechos de las personas de edad y en los derechos de las personas con discapacidad, o la lucha contra el terrorismo, entre otras.

El balance del ACNUDH fue positivo, pero se vio obligado a admitir que el gran número de agentes y procesos integrantes del sistema de DDHH que se ocupan de cuestiones relativas a la tecnología digital puede ser fuente de solapamientos y, en ocasiones, tensiones si los esfuerzos de coordinación no son suficientes. En los últimos años se ha dedicado, en exclusiva o en lo fundamental, un número cada vez mayor de resoluciones a cuestiones relativas a la tecnología digital, incluida la IA. Aunque se trata de un indicio positivo de que cada vez se presta más atención, cabe mencionar riesgos como la duplicación de esfuerzos, la merma de los escasos recursos y la ambigüedad o falta de claridad, algo que ocurre cuando las iniciativas abordan cuestiones conexas de maneras distintas.

El ACNUDH recomendó establecer un servicio de asesoramiento sobre los DDHH en el espacio digital a fin de ayudar a los Estados miembros y a las partes interesadas a integrar los DDHH en el diseño, el desarrollo, el funcionamiento, el uso y la reglamentación de las tecnologías digitales. También solicitó que se estudien y adopten medidas adecuadas para mejorar el debate y la coordinación entre los mecanismos de DDHH de NNUU a fin de respaldar la complementariedad y la coherencia de su labor en el ámbito de las tecnologías digitales. Por ejemplo, los titulares de mandatos

de los procedimientos especiales podrían mejorar la coordinación de su labor en materia de tecnologías digitales, en particular creando un grupo de coordinación. También pidió que se mejore la infraestructura de gestión de la información en todo el ecosistema de DDHH de NNUU. Otra de sus recomendaciones fue que se intensifiquen los esfuerzos por garantizar que los DDHH se tengan plenamente en cuenta en todos los ámbitos normativos relacionados con la gobernanza de las tecnologías digitales, como el comercio tradicional y electrónico, la propiedad intelectual, el derecho de la competencia, la paz y la seguridad, la ciberdelincuencia y la ciberseguridad.

V. UNESCO

La UNESCO con su experiencia en creación de estándares de ciencia e innovación se interesó pronto por el impacto de la IA. La Conferencia General de la UNESCO adoptó por aclamación su Recomendación sobre la Ética de la Inteligencia Artificial en noviembre de 2021, la cual se considera el primer marco normativo universal sobre ética de la IA. Si bien no es jurídicamente vinculante, su valor estriba en que muestra el consenso de la comunidad internacional en la materia al ser adoptado por los 193 Estados miembros de la organización. El primer borrador lo realizó un grupo de expertos y se sometió a consulta pública.

Entre sus objetivos está proteger, promover y respetar los DDHH y las libertades fundamentales, la dignidad humana y la igualdad, incluida la igualdad de género; salvaguardar los intereses de las generaciones presentes y futuras; preservar el medio ambiente, la biodiversidad y los ecosistemas; y respetar la diversidad cultural en todas las etapas del ciclo de vida de los sistemas de IA. La larga recomendación que ocupa 30 páginas en su versión en español, tiene los DDHH como uno de sus ejes principales con multitud de menciones a los mismos y está organizada en torno a una enumeración de valores (el primero de los cuales es el respeto, protección y promoción de los DDHH, las libertades fundamentales y la dignidad humana), principios[46] y ámbitos de acción política que son: evaluación del impacto ético, gobernanza y administración éticas, política de datos, desarrollo y cooperación internacional, medio ambiente y ecosistemas, género, cultura, educación e investi-

46. Estos principios son: proporcionalidad e inocuidad; seguridad y protección; equidad y no discriminación; sostenibilidad; derecho a la intimidad y protección de datos; supervisión y decisión humanas; transparencia y explicabilidad; responsabilidad y rendición de cuentas; sensibilización y educación; y gobernanza y colaboración adaptativas y de múltiples partes interesadas. Como se ve, estos principios mezclan DDHH con otro tipo de elementos relevantes.

gación, comunicación e información, economía y trabajo, salud y bienestar social. Se trata de un documento ambicioso que toca muchos elementos y hace muchas recomendaciones. No obstante, VEALE *et al*. han criticado las recomendaciones de varias organizaciones internacionales, usando como ejemplo ésta y la de la OCDE, diciendo que, en su mayor parte, no difieren significativamente de los documentos de la industria ni, posiblemente, de sus intereses, porque a pesar de su relevancia política global, el poder digital parece ser un tema que las empresas tecnológicas se esfuerzan por mantener fuera de la mesa[47].

Si bien de nuevo se trata de *soft law,* como las recomendaciones de la AGNU, según GARRIDO, se negoció de manera tan detallada que su calidad difiere en gran medida de las simples resoluciones o declaraciones.[48] Además, se ha intentado asegurar que se llevará a la práctica a través de diferentes mecanismos, al final la propia recomendación incluye varios apartados sobre: seguimiento y evaluación, aplicación y promoción de la recomendación. La Recomendación busca tener una aplicación más fácil en la práctica con dos herramientas, la Evaluación del Impacto Ético (EIE) y la Metodología de Evaluación de Preparación (RAM, por sus siglas en inglés) que fueron lanzadas en 2022.

La EIE tiene como objetivo ayudar a las partes interesadas en la IA a evaluar el impacto que los conjuntos de datos, los marcos conceptuales y los algoritmos pueden tener en la sociedad. Esta herramienta se dirige a los desarrolladores de sistemas de IA y busca apoyar el ajuste de los algoritmos para abordar o mitigar los posibles impactos negativos[49].

MANTELERO ha criticado que la EIE presenta varios problemas, especialmente destaca que se utilizan varias variables sin aclarar cómo se combinan en el impacto general[50]. Para perfeccionarla y adaptarla a su uso práctico, la UNESCO y GobLab UAI realizaron una prueba piloto de la herramienta en América Latina, trabajando con instituciones públicas y privadas para recopilar retroalimentación crítica. Entre los participantes se encontraban la Alcaldía de Bogotá, que aplicó el EIA a Chatico, una plataforma de ser-

47. VEALE *et al. op. cit.,* p. 262.
48. GARRIDO REBOLLEDO, V. "Impact of the artificial intelligence on international relations: towards a global algorithms governance", *Revista UNISCI*, núm. 67 (2025).
49. Véase Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence https://unesdoc.unesco.org/ark:/48223/pf0000386276
50. MANTELERO, A., "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template", *Computer Law & Security Review,* núm. 54 (2024).

vicios ciudadanos basada en IA, analizando su impacto en la privacidad, la transparencia y la gobernanza; Excelsis, una consultora tecnológica privada paraguaya asociada a CISOFT, que probó el EIA en un *chatbot* de IA generativa diseñado para la gestión de datos corporativos, identificando desafíos relacionados con la interoperabilidad, la alineación regulatoria y la adopción por parte del sector empresarial; finalmente, cinco instituciones peruanas, coordinadas por la Secretaría de Gobierno y Transformación Digital, evaluaron sistemas de IA en áreas como educación, certificación ambiental, agricultura y regulación energética, enfatizando la necesidad de adaptación contextual, modularidad e integración institucional[51].

Por otra parte, la RAM ayudará a los Estados a identificar su situación en relación con la Recomendación[52]. Se parte de que los Estados miembros se encuentran en diferentes niveles de preparación con respecto al desarrollo, la adopción y el uso de la IA, y pretende ayudar a los gobiernos a afinar los mecanismos de regulación y convertir los valores y principios en políticas. Se trata de una herramienta práctica que ayuda a los países a comprender el estado actual y su nivel de preparación para la implementación ética y responsable de la IA[53]. La RAM abarca cinco dimensiones:

1. Legal/regulatoria: Aborda la capacidad institucional y humana de los Estados miembros para implementar la Recomendación y gestionar las principales transformaciones sociales que desencadenaría una mayor adopción de la IA en todos los sectores de la economía. Esto incluye marcos regulatorios adecuados, así como mecanismos de monitoreo y evaluación.

2. Social/cultural: Considera los factores relevantes para el desarrollo y la implementación éticos de la IA, por ejemplo, la inclusión, la diversidad social y cultural, y la concienciación pública. También aborda las actitudes hacia las tecnologías de IA, incluida la aceptación pública, para ayudar a revelar los valores y preferencias sociales que rigen las decisiones sociales.

---

51. BAYTELMAN, P., GARRIDO, R., ORREGO, G., GERMAN, M., y TABARES, R., "Piloting the Ethical Impact Assessment (EIA) in Latin America", *UNESCO*, 11/03/2025 https://www.unesco.org/en/articles/piloting-ethical-impact-assessment-eia-latin-america
52. Véase Metodología de evaluación del estadio de preparación. Una herramienta de la Recomendación sobre la Ética de la Inteligencia Artificial https://unesdoc.unesco.org/ark:/48223/pf0000385198_spa
53. RAMOS, G., SQUICCIARINI, M., y LAMM, E, "Making AI Ethical by Design: The UNESCO Perspective", *Computer* vol. 57, núm. 2 (2024), pp. 33-43.

3. Económica: Su objetivo es abordar el tamaño y la solidez de la oferta del ecosistema de IA en el país, así como su capacidad para desarrollar soluciones de IA que reflejen las necesidades y condiciones específicas.

4. Científica/educativa: Evalúa la investigación y el desarrollo de IA realizados en un país (por ejemplo, publicaciones y patentes relacionadas con IA, investigadores e ingenieros de IA que participan en I+D). También analiza la investigación sobre ética de la IA y la disponibilidad de oportunidades educativas para estudiantes y el público en general. Además, monitorea el número de estudiantes (graduados) y profesionales en IA, TIC o disciplinas STEM, así como el nivel de IA y de cibercompetencias en la población.

5. Técnica/infraestructural: Evalúa el nivel de TIC e infraestructura técnica relacionada existente y refleja la idea de que, sin la infraestructura pertinente, no es posible ampliar el desarrollo de la IA ni la implementación de soluciones basadas en IA.

UNESCO colabora actualmente con más de 50 países de todo el mundo para implementar el RAM y continuará ampliando esta labor para fortalecer su impacto global.

La aplicación de la Recomendación se complementa con una serie de iniciativas y redes: el Grupo de Expertos de Alto Nivel sobre la Aplicación de la Recomendación para ayudar a desarrollar herramientas y metodologías innovadoras; el Foro Mundial sobre la Ética de la IA como punto central para debatir los retos de estas tecnologías; el Observatorio Mundial de la Ética de la IA como plataforma digital para informar sobre las políticas en este ámbito y los avances sobre el terreno; los Expertos en Ética de la IA sin fronteras para su despliegue en los Estados miembros en función de las necesidades para ayudar a la aplicación, especialmente en los países en desarrollo; la Red mundial de centros de conocimiento sobre la ética de la IA, que moviliza a las principales universidades y centros académicos del mundo para apoyar la creación de capacidades y la investigación sobre la ética de la IA; y la Red de Mujeres por la Ética de la IA, que moviliza a destacadas defensoras de la igualdad de género para la aplicación de la política de género de la Recomendación[54].

Respecto a sectores concretos, en 2022, UNESCO lanzó una Encuesta de Evaluación de Necesidades de Inteligencia Artificial en África y el 90% de

54. Véase Recomendación sobre la Ética de la Inteligencia Artificial — UNESCO Biblioteca Digital, https://unesdoc.unesco.org/ark:/48223/pf0000385198_spa

los países encuestados solicitaron apoyo para el desarrollo de capacidades en IA para el poder judicial. Para ello se elaboró el *Global toolkit on AI and the rule of law for the judiciary*[55] y en 2024 también se lanzaron las Directrices de la UNESCO para el uso de sistemas de inteligencia artificial en juzgados y tribunales. La persona encargada de su redacción, aunque han sido revisadas por un gran número de expertos, ha sido Juan David Gutiérrez, Profesor de la Universidad de los Andes, por lo que no es de extrañar que el primer país que ha adaptado su legislación a la mismas ha sido Colombia[56].

VI. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

La UIT no pudo tener todo el protagonismo que le gustaría en el marco de la gobernanza de Internet,[57] por lo que en relación con la GIA decidió tomar rápidamente la iniciativa con algo que sí había hecho con éxito en ese ámbito que era buscar la coordinación con otras agencias de NNUU[58]. Lanzó en alianza con otros 40 órganos de NNUU la plataforma Inteligencia Artificial para el Bien (*AI for Good*) que lidera. Algunos de sus resultados más destacados son sus cumbres anuales, y la puesta en marcha su repositorio de IA a fin de detectar las aplicaciones responsables y prácticas de la IA para promover los ODS[59]. A nivel más técnico ha dado lugar a la Iniciativa

55. Sus autores son STANKOVICH, M., FELDFEBER, I., QUIROGA, Y., CIOLFI FELICE, M. y VUKOSI, M. https://unesdoc.unesco.org/ark:/48223/pf0000387331
56. La justicia se une a la innovación: las revolucionarias directrices de IA de Colombia para los tribunales https://www.unesco.org/es/articles/la-justicia-se-une-la-innovacion-las-revolucionarias-directrices-de-ia-de-colombia-para-los Sobre el uso de la IA en este sector en Iberoamérica véase, LAFUENTE TORRALBA, A., "Fabulas de robots en el mundo judicial (o del uso de la inteligencia artificial en la justicia europea e iberoamericana)", en *El Derecho y la inteligencia artificial*, coords. MONTEJO RIVERO y AMOROSO FERNÁNDEZ (en prensa).
57. RADU, R., *Negotiating internet governance*. Oxford University Press, 2019, p. 130.
58. KURBALIJA, J., *An introduction to internet governance*. Diplo Foundation, 7.ª ed., 2016, p. 238.
59. Dentro de la labor de NNUU en este ámbito ha elaborado informes donde se puede ver toda la panoplia de actividades de la organización, por ejemplo, en 2023, 47 entidades desarrollaron 408 proyectos. Se mantiene un fuerte enfoque en los ODS 9 (Industria, Innovación e Infraestructura), 10 (Reducción de las Desigualdades), 16 (Paz, justicia e instituciones sólidas) y 17 (Alianza para el logro de los Objetivos), junto con el ODS 13 (Acción por el Clima). Se requiere un mayor enfoque en los ODS 6 (Agua Limpia y Saneamiento), 7 (Energía Asequible y No Contaminante), 12 (Consumo y producción responsables), 14 (Vida Submarina) y 15 (Vida de Ecosistemas Terrestres). La colaboración entre múltiples partes interesadas sigue siendo una prioridad para el sistema de las NNUU. Casi el 60% de los proyectos de NNUU han reportado colaboraciones con el sistema de NNUU, el sector privado, los gobiernos, la sociedad

Global sobre IA y Datos Comunes y *focus groups* previos a la estandarización sobre IA y Salud (con la OMS), IA y Conducción Autónoma y Asistida, IA y Eficiencia Ambiental, IA y Gestión de Desastres Naturales (con la Organización Meteorológica Internacional y el PNUMA), Aprendizaje Automático y 5G, IA e Internet de las Cosas para la Agricultura Digital (con la FAO) y la Iniciativa de IA para la Seguridad Vial.

VII. CONCLUSIONES

Como se ha podido observar en este capítulo, las NNUU llevan varios años desarrollado una labor muy intensa en el campo de la GIA, especialmente desde una perspectiva de DDHH. En 2025, veremos la cristalización de las recomendaciones del HLAB y del Pacto Digital Mundial con la creación del Panel Científico Internacional Independiente sobre Inteligencia Artificial y del Diálogo Mundial sobre la Gobernanza de la Inteligencia Artificial. Estas iniciativas responden a la necesidad de enfrentar los retos de la IA desde una perspectiva científicamente informada y multipartita. Es relevante que esto ocurra al nivel de NNUU para que las preocupaciones del Sur Global sean escuchadas y no permanezcan al margen de la toma de decisiones internacional que afecta a estas cuestiones. No obstante, las propuestas de gobernanza no son muy creativas puesto que replican modalidades utilizadas en otros ámbitos, sin tener excesivamente en cuenta las particularidades de la IA. Por ejemplo, cabe plantearse qué va a aportar el Diálogo más allá de los foros internacionales ya existentes sobre la materia, por eso será interesante evaluar su utilidad real y su valor añadido, así como el de los primeros informes del Panel. Cabe destacar el papel de España en la materia, con un miembro español del HLAB y coliderando la creación del Panel y el Diálogo.

Las resoluciones sobre la materia de la AGNU en 2024 presentan un panorama interesante en el que se aprecian los puntos de convergencia en la materia con un énfasis importante en los DDHH, pero también en la necesidad de apoyar a los Estados del Sur Global para que no pierdan oportunidades de desarrollo y ésta no sea una nueva fuente de desigual-

---

civil, el mundo académico o con otra organización internacional, lo que demuestra el enfoque de NNUU en mantener alianzas sólidas con las partes interesadas internas y externas. Los resultados más comunes del trabajo del sistema de NNUU sobre IA siguen siendo informes y herramientas de software como aplicaciones móviles o web, paneles de búsqueda y *chatbots* basados en IA generativa. Además, alrededor del 13 % indicó centrarse en la creación de bases de datos. Véase UIT, *United Nations Activities on Artificial Intelligence (AI) 2023*, 2024.

dad. En ese sentido, China se ha erigido en un líder mundial, un espacio que además ha abandonado Estados Unidos que tras encabezar la primera resolución se ha replegado sobre sí mismo con la Administración Trump más partidaria de la desregulación. También resulta evidente que es más difícil llegar a acuerdos en materia militar dado que la resolución sobre esa materia fue la única que no se pudo adoptar por asentimiento, a pesar de no ser excesivamente ambiciosa. En ese sentido, la UNESCO ha llevado a cabo un trabajo muy intenso para llevar a la práctica su recomendación sobre la ética de la IA, buscando que no se quede en meras palabras. Esta organización junto con la UIT tiene un rol especialmente relevante en el trabajo de las NNUU en la materia.

Es evidente que la IA afecta al ejercicio de múltiples derechos por lo que es importante que la Oficina del ACNUDH tenga la capacidad técnica para pronunciarse sobre estas cuestiones y coordine la actuación de los relatores especiales y pueda también ofrecer recomendaciones y apoyo a los Estados para regular la IA con las necesarias salvaguardas de DDHH. Las NNUU enfrentan estos retos en un contexto de recortes presupuestarios lo que sin duda dificultará su trabajo, pero esta es una de las prioridades del SGNU para 2025.

BIBLIOGRAFÍA

ADAMS, R., "AI Is Bad News for the Global South", *Foreign Policy*, 17/12/2014. https://foreignpolicy.com/2024/12/17/ai-global-south-inequality/

ADAN, S. N., TRAGER, R., BLOMQUIST, K., DENNIS, C., EDOM, G., VELASCO, L., ABUNGU, C., GARFINKEL, B., JACOBS, J., OKOLO, C. T., WU, B. y VIPRA, J., *Voice and Access in AI: Global AI Majority Participation in Artificial Intelligence Development and Governance*, Oxford Martin School of AI Governance White Paper, 2024.

ASSAAD, Z., "The United Nations has a plan to govern AI — but has it bought the industry's hype?", *The Conversation*, 23/09/2024, https://theconversation.com/the-united-nations-has-a-plan-to-govern-ai-but-has-it-bought-the-industrys-hype-239494

BACKOVSKY, D. y BRYSON, J.J., "Going Nuclear? Precedents and Options for the Transnational Governance of AI", *Horizons: Journal of International Relations and Sustainable Development*, núm. 24 (2023), pp. 84-95.

BAYTELMAN, P., GARRIDO, R., ORREGO, G., GERMAN, M., y TABARES, R., "Piloting the Ethical Impact Assessment (EIA) in Latin America", *UNESCO*, 11/03/2025 https://www.unesco.org/en/articles/piloting-ethical-impact-assessment-eia-latin-america

BELLI, L. y GASPAR, W. B., "AI from the global majority: What are we debating and why?", *AI from the global majority*, FGV Direito Rio, pp. 19-28.

CASTELLÓ PASTOR, J. J., "Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea". *Cuadernos de Derecho Transnacional*, vol. 17, núm. 1 (2025), pp. 308-328.

COLOMINA SALÓ, C. y GALCERAN-VERCHER, M., "Las otras geopolíticas de la inteligencia artificial", *Revista CIDOB d'afers internacionals,* vol. 138 (2024), pp. 27-50.

FAJARDO DEL CASTILLO, T., *El soft law en el Derecho Internacional y Europeo: Su capacidad para dar respuesta a los desafíos normativos actuales*, Tirant Lo Blanch, 2024.

FATAFTA, M. y LEUFEUR, D., "Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes", *Access Now*, 9/05/2024 https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/

FOURNIER-TOMBS, E., SIDDIQUI, M., CASTETS-RENARD, C. y NDIOR, V., *A Global Architecture for Artificial Intelligence*, United Nations University Centre for Policy Research, Technical Note, 2023.

GARRIDO REBOLLEDO, V., "Impact of the artificial intelligence on international relations: towards a global algorithms governance", *Revista UNISCI,* núm. 67 (2025).

GASCÓN MARCÉN, A., "Derechos humanos e inteligencia artificial" en *Setenta años de Constitución Italiana y cuarenta años de Constitución Española*, Vol. 5 (Retos en el siglo XXI), Centro de Estudios Políticos y Constitucionales y BOE, 2020, pp. 335-350.

GASCÓN MARCÉN, A., "El Sur Global y la pugna por la regulación digital internacional" (pendiente de publicación 2025).

GASCÓN MARCÉN, A., "La diligencia debida en los Reglamentos de Servicios Digitales e Inteligencia Artificial", *Empresa y derechos humanos: retos*

y tendencias normativas ante un complejo e inédito contexto geoestratégico, Aranzadi La Ley, 2025, pp. 231-250.

GASCÓN MARCÉN, A., "La gobernanza de la inteligencia artificial en Estados Unidos y China, modelos regulatorios alternativos al europeo", en *Actualidad legislativa y jurisprudencial: el Derecho ante el reto de las tecnologías disruptivas*, Colex, 2025.

GASCÓN MARCÉN, A., "La propuesta de Reglamento de la Comisión Europea por el que se establecen normas armonizadas en materia de inteligencia artificial", en *Retos de la sociedad digital: Regulación y fiscalidad en un contexto internacional*, Reus, 2022, pp. 11-36.

GASCÓN MARCÉN, A., "Nuevo Convenio Marco sobre Inteligencia Artificial del Consejo de Europa", *Derecho Digital e Innovación. Digital Law and Innovation Review*, núm. 20 (2024).

GMYREK, P., WINKLER, H. y GARGANTA, S., *Buffer or Bottleneck? Employment Exposure to Generative AI and the Digital Divide in Latin America*, World Bank/International Labour Organization, 2024.

HAUSENLOY, J. y DENNIS, C., *Towards a UN Role in Governing Foundation Artificial Intelligence Models,* United Nations University Centre for Policy Research, Working Paper, 2023.

KNAUER, A., "The First United Nations General Assembly Resolution on Artificial Intelligence", *EJIL:Talk!,* 2/04/2024 https://www.ejiltalk.org/the-first-united-nations-general-assembly-resolution-on-artificial-intelligence/

KURBALIJA, J., An introduction to internet governance. Diplo Foundation, 7.ª ed., 2016.

LAFUENTE TORRALBA, A., "Fabulas de robots en el mundo judicial (o del uso de la inteligencia artificial en la justicia europea e iberoamericana)", en *El Derecho y la inteligencia artificial*, coords. MONTEJO RIVERO y AMOROSO FERNÁNDEZ (en prensa).

LAHMANN, H., "Gaza and the Collective Political Costs of Algorithmic Warfare", *EJIL:Talk!,* 25/03/2025 https://www.ejiltalk.org/gaza-and-the-collective-political-costs-of-algorithmic-warfare/

MANTELERO, A., "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template", *Computer Law & Security Review*, núm. 54 (2024).

OKOLO, C. T., "AI in the Global South: Opportunities and challenges towards more inclusive governance", *Brookings,* 1/11/2023 https://www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challenges-towards-more-inclusive-governance/

RADU, R., *Negotiating internet governance.* Oxford University Press, 2019.

RAMOS, G., SQUICCIARINI, M., y LAMM, E, "Making AI Ethical by Design: The UNESCO Perspective", *Computer* vol. 57, núm. 2 (2024), pp. 33-43.

ROBLES CARRILLO, M., "La gobernanza de la inteligencia artificial: contexto y parámetros generales", *Revista Electrónica de Estudios Internacionales,* núm. 39 (2020).

RODRÍGUEZ, J. M., "La regulación de la inteligencia artificial y la responsabilidad de los Estados en su utilización militar", *Revista UNISCI*, núm. 67 (2025), pp. 53-86.

SMUHA, N., "From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence", *Law, Innovation and Technology*, vol. 13, núm. 1 (2021), pp. 57-84.

STANDFORD, *AI Index Annual Report 2024*, 2024.

TIMCKE, S., "Response to the Governing AI for Humanity Report", *TechPolicy.Press*, 26/09/2024 https://www.techpolicy.press/deficits-gaps-and-compromises-in-the-uns-governing-ai-for-humanity/

UIT, *United Nations Activities on Artificial Intelligence (AI) 2023*, 2024.

VEALE, M., MATUS, K., y GORWA, R., "AI and global governance: modalities, rationales, tensions", *Annual Review of Law and Social Science*, vol. 19, núm. 1 (2023), pp. 255-275.

BLOQUE III

Capítulo 10

La propiedad digital y su sucesión *mortis causa*: ¿nuevos escenarios para el Derecho internacional privado europeo?*

Isabel Antón Juárez
Prof.ª Titular de Derecho Internacional Privado
Universidad Carlos III de Madrid
ORCID ID: 0000-0002-5639-2301

SUMARIO: I. APROXIMACIÓN INICIAL. II. HACIA UN CONCEPTO DE "BIEN DIGITAL". III. EL IMPACTO DE LA VIDA DIGITAL EN LA SUCESIÓN MORTIS CAUSA: ¿TODA SUCESIÓN ES INTERNACIONAL? 1. *Aproximación inicial*. 2. *La calificación de la sucesión* mortis causa *como internacional por la existencia de bienes digitales*. 3. *Las normas que regulan la sucesión* mortis causa *transfronteriza de bienes digitales*. IV. LA CATEGORIZACIÓN DE LOS BIENES DIGITALES. V. LA DETERMINACIÓN DE LA COMPETENCIA JUDICIAL INTERNACIONAL Y EL DERECHO APLICABLE DE LA SUCESIÓN MORTIS CAUSA DE BIENES DIGITALES. 1. *El punto de partida*. 2. *Los diferentes escenarios*. 3. *La determinación del Derecho aplicable bienes personales y mixtos*. 4. *Los litigios derivados de la sucesión* mortis causa *de bienes digitales y la determinación del tribunal competente.* VI. LA SUCESIÓN DE BIENES DIGITALES CREADOS POR EL CAUSANTE. VII. REFLEXIONES FINALES. BIBLIOGRAFÍA.

I. APROXIMACIÓN INICIAL

Nuestra presencia en Internet es innegable en la actualidad. Según muestran las estadísticas en un informe del año 2023, en España, sólo un 3,37 %

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro la autora.

de la población nunca habría accedido a la red de redes[1]. Es más, si se compara con datos del año 2010, se puede apreciar cómo ha ido decreciendo la cifra desde entonces, ya que, en aquel momento, un tercio de la población española nunca se había conectado a Internet[2]. De hecho, si se atiende a datos sobre el acceso y uso a Internet en los países europeos puede apreciarse como de media sólo un 5,97 nunca habría accedido a Internet en Europa[3]. Estos datos muestran que entre los 27, hay Estados como Luxemburgo en los que sólo un 0,45 de su población nunca se habría conectado a Internet[4]. Estas estadísticas muestran como el uso de Internet está más que presente en nuestros quehaceres diarios, impactando su uso en otras esferas de nuestra vida física e incluso una vez que morimos.

El uso de Internet presenta múltiples consecuencias y una de ellas es que generamos un importante número de datos e información sobre nosotros y sobre lo que hacemos en la red mientras navegamos. Mucha de esa información que generamos es visible y notoria porque las personas nos ocupamos de hacerla pública mediante una foto o comentario en una red social. Sin embargo, hay otra información, que no es pública, bien porque guarda relación con el rastro que dejamos al navegar mediante las *cookies* que aceptamos, bien porque nosotros mismos hemos decidido no comunicarla, por ejemplo, una cuenta en una plataforma que permite que tengamos un monedero de criptoactivos. Todo este contenido que creamos en Internet de forma individual se denomina "huella digital".

La cuestión que perseguimos abordar en el presente trabajo es qué sucede con toda esa información que se genera en Internet cuando una persona fallece. Especialmente, nos centraremos en esa información que tiene un valor, ya sea patrimonial o personal. Pregunta fácil de plantear pero compleja de responder debido a aspectos como: i) Mucha información de la que se genera en Internet sólo la conocemos nosotros mismos; ii) Alguna tiene valor económico, pero otra, no; iii) Esa información que no tiene valor patrimonial puede tener valor pero desde una esfera más personal, dando

1. *Vid.* al respecto, "Evolución del porcentaje de personas que nunca había accedido a Internet en España de 2010 a 2023", Statista, disponible en https://es.statista.com/estadisticas/599658/porcentaje-de-personas-que-nunca-habia-utilizado-internet/ (consultado el 27 de marzo de 2025).
2. *Ibidem.*
3. *Vid.* el informe "Porcentaje de población que nunca había utilizado Internet en la Unión Europea (UE-27) en 2023", Statista, disponible en https://es.statista.com/estadisticas/599658/porcentaje-de-personas-que-nunca-habia-utilizado-internet/ (consultado el 27 de marzo de 2025).
4. *Ibidem.*

lugar a que los herederos quieran acceder a esa información tras la muerte de la persona que la ha generado, impactando de lleno en la privacidad *post mortem*; iv) El elemento extranjero está presente en la sucesión de ese posible patrimonio digital en todo caso, lo que implica que las normas de Derecho internacional privado europeo entren en escena.

La complejidad jurídica del tema a abordar se agrava debido a que no existe una normativa material al respecto en España ni en prácticamente ningún Estado miembro y tampoco desde la perspectiva internacional privatista. De hecho, la normativa material en materia sucesoria que existe no ofrece para soluciones debido a que cuando se creó no existían los problemas complejos que plantean en la actualidad la sucesión de bienes digitales[5]. La realidad es, que en la mayoría de los casos, los problemas que plantea la sucesión *mortis causa* de los bienes físicos no es la misma que plantea los bienes digitales.

Ante este escenario vamos a dividir el presente trabajo en tres partes diferenciadas: en la primera parte se abordarán cuestiones introductorias relacionadas con el concepto de bien digital, la internacionalidad de estas sucesiones *mortis causa* y la normativa que se debe tener en cuenta desde una perspectiva transnacional. En la segunda parte, el objeto del trabajo se centrará en categorizar los bienes digitales para poder determinar cómo se podrían integrar en una sucesión *mortis causa*. Y en la tercera parte, se abordarán cuestiones de litigación transfronteriza abordando qué pleitos se podrían derivar de la sucesión *mortis causa* de bienes digitales debido a que muchos de ellos tienen un carácter patrimonial pero también personal y cuál sería el Derecho aplicable a los mismos.

II. HACIA UN CONCEPTO DE "BIEN DIGITAL"

Un primer problema que aparece en la sucesión *mortis causa* de bienes digitales es determinar qué se entiende por "bien digital". Esto es así porque no hay una norma europea, ningún Reglamento europeo ni en materia de familia ni en materia patrimonial, que ofrezca una definición para este término a pesar de su importancia en la práctica.

Por lo tanto, ante esta falta de uniformidad legislativa y también jurisprudencial, la doctrina ha señalado que una forma de llegar a un concepto de

5. Para una misma visión *vid*., MASPES, I., "Morte digitale e persistenza dei diritti oltre ka vita della persona física" (Nota a ordinanza Tribunale civile Milano sezione I 9 febbraio 2021*), Giurisprudenza italiana*, 2021, fasc. 7, p. 1602.

bien digital es diferenciando su forma de procesamiento[6] o cómo se almacena esa información[7]. Así, en base a este criterio de cómo se procesan o dónde se encuentran recogidos los bienes digitales se podría diferenciar entre:

- Bienes digitales que se encuentran exclusivamente en formato on line y que se pueden representar en formato binario. Es decir, bienes digitales que representan mediante secuencias de series de números que son 0 y 1. Esto es lo que conoce como bits (*binary digit*). Una foto que realizamos con el *smartphone* y que luego subimos a una red social es un conjunto de *bits*. Un aspecto fundamental que estudiaremos más adelante es que para la creación de estos "bienes" que únicamente se encuentran en formato digital existe un contrato firmado entre el causante y el prestador de servicios digitales, es decir, la plataforma de vídeo, la red social, la empresa que ofrece servicio de correo electrónico, etc. Además, estos "bienes digitales" en realidad no son bienes en puridad sino más bien un servicio al que accede el causante de forma personal y en la mayoría de los casos será intransferible porque así lo señalan generalmente los contratos que se firman con los prestadores de estos servicios. En esta categoría de bienes digitales que se encuentran *on line* se podrían incluir cuentas en *marketplace*s, documentos almacenados en la nube, cuentas en redes sociales, correos electrónicos, contraseñas, bienes electrónicos adquiridos en línea (música, películas, *software*), monedas virtuales (bitcoin y criptomonedas), *software* y, de forma más general, datos relativos a una persona generados digitalmente e introducidos en la red[8].

- Bienes digitales que se encuentran en un soporte físico. Es decir, bienes que se almacenan en un ordenador, en CDs o memorias USB. Estos bienes digitales seguirán la suerte del soporte físico en el que se encuentren[9]. Aunque puede parecer que estos bienes digitales son más fáciles de heredar, también pueden presentar sus problemas debido a que la propiedad sobre el bien físico (ordenador, por ejemplo) en el que se almacenan los datos pueden concurrir en la

6. MASPES, I., "Morte digitale e persistenza dei diritti oltre ka vita della persona física" (Nota a ordinanza Tribunale civile Milano sezione I 9 febbraio 2021*), Giurisprudenza italiana*, 2021, fasc. 7, p. 1603.
7. Pérez Vallejo, A.M.ª /Vivas Tesón, I., *La transmisión mortis causa del patrimonio intelectual y digital*, Thomson Reuters Aranzadi, Navarra, 2022, p. 210.
8. MASPES, I., "Morte digitale e persistenza…", *op. cit.*, p. 1603.
9. *Ibidem*, p. 1603.

misma persona titular de esos bienes digitales ahí almacenados o no necesariamente[10].

Otra clasificación muy presente en la doctrina, y que se desarrollará más adelante es clasificar los bienes digitales en atención a si tienen un valor patrimonial, personal o incluso mixto.

III. EL IMPACTO DE LA VIDA DIGITAL EN LA SUCESIÓN MORTIS CAUSA: ¿TODA SUCESIÓN ES INTERNACIONAL?

1. APROXIMACIÓN INICIAL

En atención a los datos señalados anteriormente, en la actualidad, la gran mayoría de las personas tiene presencia en Internet. Esta presencia quizás sea más intensa cuanto más joven se sea, ya que la realidad es, que el acceso y uso de Internet por las diferentes generaciones que conviven en la actualidad es desigual. Esto hace que puedan existir sucesiones en las que el finado ostente una web propia, tenga varios monederos digitales en los que hay criptoactivos, cuente con varias cuentas de correo electrónico, su presencia en redes sociales haya sido activa subiendo fotos, vídeos y realizando comentarios, ostente una cuenta para realizar inversiones y tenga varios *iphone(s)* y un par de ordenadores[11]. Pero también, hoy en día, pueden existir sucesiones de personas que nacieron en torno a los años 30 del pasado siglo en las que la presencia en Internet sea escasa, tanto desde una perspectiva económica como personal y la sucesión no se vea impactada en absoluto.

Para el presente trabajo el *target* relevante de personas serán las más jóvenes y activas en los que a la creación y tenencia de activos digitales se refiere, debido a que conforme vaya pasando el tiempo, las sucesiones *mortis causa* más se verán afectadas por la vida digital que hemos llevado durante nuestra existencia.

De este modo, debido a este gran uso de Internet, tan diferente y de forma tan generalizada entre generaciones de personas con intereses tan distintos cabe plantearse dos cuestiones preliminares: 1.º) ¿Toda sucesión *mortis causa* podría calificarse como internacional debido al uso de plataformas que requieren que el usuario firme condiciones generales de contratación con empresas cuyas sedes se encuentran en terceros países como EE.UU.?;

10. Pérez Vallejo, A.M.ª /Vivas Tesón, I., *La transmisión mortis…, op. cit.*, pp. 227-228.
11. Sobre esa diferencia entre generaciones en el uso de Internet y que conviven en la actualidad *vid*. Pérez Vallejo, A.M.ª /Vivas Tesón, I., *La transmisión mortis causa del patrimonio intelectual y digital*, Thomson Reuters Aranzadi, Navarra, 2022, p. 204.

2.º) ¿Actualmente existen soluciones uniformes sobre cómo se integra el patrimonio digital en una sucesión *mortis causa*?

2. LA CALIFICACIÓN DE LA SUCESIÓN *MORTIS CAUSA* COMO INTERNACIONAL POR LA EXISTENCIA DE BIENES DIGITALES

En relación a la primera cuestión que surge y que es necesario resolver al plantearse la sucesión por causa de muerte del patrimonio digital de una persona es si toda sucesión debería calificarse de internacional. En otras palabras, debido a que las empresas que nos ofrecen toda esa vida paralela en Internet tienen sus sedes en el extranjero[12] y para poder acceder al contenido o servicios que ofrecen hay que firman contratos con ellas, este hecho puede implicar que una sucesión *mortis causa* que presenta todos sus elementos conectados con un único país puede cambiar a transnacional como consecuencia del patrimonio digital. Desde nuestra visión, la respuesta es no. Por el hecho de ostentar un patrimonio digital, ubicuo y en el que intervienen empresas radicadas en diferentes países que dan acceso a un servicio digital, una sucesión enteramente nacional cuyos elementos se ubican en un único Estado no sería internacional[13]. Los motivos para esta posición podrían basarse en: 1) La razón de ser del Derecho internacional privado; 2) Lo establecido por las normas potencialmente aplicables como el *Reglamento (UE) n.º 650/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a la competencia, la ley aplicable, el reconocimiento y la ejecución de las resoluciones, a la aceptación y la ejecución de los documentos públicos en materia*

12. En el caso de las redes sociales (la empresa *Meta* con sede en California (EE.UU.) es dueña de Facebook, Instagram y WhatsApp; la empresa Microsoft de la red social profesional *Linkedin* tiene su sede estatutaria en Washington (EE.UU.); *Tik Tok* pertenece a la empresa china *Bytedance* con sede en Pekín).A la hora de comprar en Internet y tener cuentas en *ecommerce, Amazon* (con sede en Seatle y Arlington, ambas ciudades estadounidenses) o *Alibaba* (cuya sede se encuentra en Hangzou, China), destacan sobre el resto; cuentas de *email como* es el caso de *Gmail*, cuya sede se encuentra en California (EE.UU.); cuentas de criptoactivos que se pueden guardar en monederos virtuales como los que ofrecen plataformas como *Binance*, cuya sede se encuentra en Malta; la creación de vídeos o la tenencia de cuentas en plataformas como *YouTube*, con sede en California (EE.UU.); simplemente almacenamos contenido en la red mediante plataformas como Dropbox, cuya sede también se encuentra en California (EE.UU.), nos divertimos escuchando música en *Spotify* (empresa con sede en Suecia) o viendo series o películas en Netflix (con headquarters en la ciudad de Los Gatos,California, EE.UU.) o HBO (cuya sede estatutaria se encuentra en Nueva York).

13. *Vid.* en este sentido, VARIENGO, I./ RE, J., "Managing managing cross-border 'digital Succession' in the digital era: preliminary remarks on the new challenges for the current legal framework", *EU and comparative law issues and challenge series*, Special issue — Law in the age of modern technologies, Vol. 7 (2023), p. 40.

de sucesiones mortis causa y a la creación de un certificado sucesorio europeo (en adelante, RES[14]); 3) La relevancia de la seguridad jurídica.

En relación a los objetivos y razón de ser del Derecho internacional privado hay que tener presente que esta disciplina se ocupa de determinar el tribunal competente, el derecho aplicable y los efectos de las resoluciones judiciales en un país diferente de donde se dictan respecto de las relaciones privadas en las que existe uno o varios elementos extranjeros[15]. Estos elementos extranjeros deberían estar localizados en diferentes Estados, entendido como territorios físicos geográficamente diferentes para poder considerar que estamos ante una sucesión transfronteriza[16]. Hay doctrina, y también el propio TJUE, que ha apoyado que en determinadas situaciones que, con un simple elemento extranjero, siendo indiferente su relevancia es suficiente para calificar una situación como privada internacional sin necesidad de que estén implicados en la situación varios Estados miembros[17]. Esta tesis es la que se conoce como "la tesis del elemento extranjero puro"[18]. Sin embargo, en el caso de las sucesiones *mortis causa* si analizamos lo dispuesto por el TJUE[19] para determinar en qué casos una sucesión es transfronteriza a efectos del RES podemos apreciar que es necesario que existan diferentes elementos extranjeros que conecten la sucesión con más de un Estado[20].

14. DOUE núm. 201, de 27 de julio de 2012.
15. Sobre este particular *vid. ad ex.* CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, pp. 158-164.
16. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit*., p. 39.
17. STJUE de 14 de noviembre de 2013, C-478/12, *Maletic*, ECLI:EU:C:2013:735, apartado 26.
18. CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, p. 137.
19. STJUE de 21 de julio de 2018, C-20/17, *Oberle*, ECLI:EU:C:2018:485, apartado 32. Para un análisis sobre esta sentencia, *vid. ad ex*., CASTELLANOS RUIZ, M.J., "Competencia internacional en materia de expedición de certificados sucesorios: a propósito de la Sentencia del TJUE 21 junio 2018, Vincent Pierre Oberle, C-20/17", *Cuadernos de Derecho Transnacional (CDT)*, vol. 12, n.º 1, 2020, pp. 473-511; GÓMEZ-RIESCO TABERNERO DE PAZ, J., "Réflexions sur la notion de 'juridiction' au sens de l'Article 3.2 du Règlement (UE) n.º 650/2012 après les arrêts de la Cour de Justice de l'Union Européenne Oberle, C-20/17, et WB, C-658/17. Perspective espagnole", *Cuadernos de Derecho Transnacional (CDT)*, vol. 12, n.º 2, 2020, pp. 1001-1019.
20. El legislador europeo pudo definir en el texto del RES cuando una sucesión *mortis causa* se debe considerar transfronteriza pero no lo hizo. La doctrina apunta que esa omisión se debe a que si otorgaba una definición se podía dejar asuntos fuera. Es decir, por el temor de no poder ofrecer una solución general, el legislador prefirió no definir qué es una sucesión *mortis causa* transfronteriza a la luz del RES. Así, el legislador prefirió que ese concepto se fuera construyendo en atención a la aplicación del RES por parte de autoridades y tribunales Sobre este particular, *vid*. CARRASCOSA GONZÁLEZ, J., *El Reglamento sucesorio europeo: análisis crítico*, Rapid centro color, Murcia, 2019, p. 66.

Esto puede ser bien porque los bienes que componen la sucesión *mortis causa* se encuentren en diferentes Estados o el Estado de la nacionalidad del causante no coincide con el país de su residencia habitual al momento del fallecimiento. De este modo, para calificar una sucesión como transfronteriza se necesita que la misma tenga tal repercusión[21], y desde nuestro punto de vista, esto es algún elemento más que el contrato que firma el causante con la plataforma que va a prestar los servicios de vídeo en *streaming* o que le va a permitir hacer compras en un *ecommerce*. Si con ese simple elemento extranjero fuera suficiente, en la actualidad, prácticamente todas las sucesiones *mortis causa* serían transfronterizas lo que daría lugar a una importante inseguridad jurídica para los herederos debido a que se suscitaría importantes dudas de cuál sería el Derecho aplicable a la sucesión.

3. LAS NORMAS QUE REGULAN LA SUCESIÓN *MORTIS CAUSA* TRANSFRONTERIZA DE BIENES DIGITALES

En relación con la segunda cuestión preliminar que nos planteábamos, si existen soluciones uniformes en materia de Derecho internacional privado a nivel europeo de cómo se integraría en la sucesión *mortis causa* el patrimonio digital, la respuesta es no. Hay que tener presente que la norma potencialmente aplicable a una sucesión *mortis causa* de patrimonio digital sería el RES debido a que, aunque no recoge nada sobre bienes digitales, es la normativa directamente aplicable por tribunales y autoridades europeas en la UE a las sucesiones *mortis causa* transfronterizas. Además, este Reglamento europeo se basa en el principio de unidad de la sucesión[22], siendo aplicable tanto a bienes muebles e inmuebles[23] por lo que si los bienes digitales fueran unos bienes más dentro de una sucesión *mortis causa* también deberían quedar incluidos en el RES en atención al citado principio[24].

Junto con el RES, otra norma relevante a tener presente con relación al objeto del presente trabajo es el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas*

21. En la jurisprudencia *vid*. STJUE de 16 de julio de 2020, C-80/19, E.E. vs. K.D, ECLI:EU:C:2020:569, apartados 45. En la doctrina *vid*. CASTELLANOS RUIZ, E., "Sucesión hereditaria.El Reglamento Sucesorio europeo", en CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, pp. 2374-2376.
22. Davì, A., "Il nuovo diritto internazionale privato delle successioni nell'Unione Europea", *Cuadernos de Derecho Transnacional*, vol. 5, n.º 2, 2013, p. 25.
23. Considerando 15 RES.
24. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit*., p. 41.

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 (en adelante, RGPD). Esta norma es importante debido a que una de las dificultades que presenta la sucesión *mortis causa* de bienes digitales es la estrecha conexión que presentan con los derechos de la personalidad. Así, algunos bienes digitales no sólo ostentan una naturaleza patrimonial, sino que también tienen una vertiente personal que afecta de lleno a la privacidad de las personas. Y a pesar de que el RGDP, en atención a su considerando 27, no se aplicaría a la protección de los datos personales de las personas fallecidas, ese mismo considerando permite que los Estados miembros puedan desarrollar normativa para la protección de la privacidad *post mortem*[25]. Y así se ha hecho. Como ejemplo, podemos poner de manifiesto, los arts. 3 y 96 de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*[26] (en adelante, Ley española de protección de datos personales). El art. 3 (el cual es una excepción al art. 2.2 b) recogido también en la citada Ley española) establece la protección de los datos personales de las personas fallecidas y el art. 96 se ocupa de desarrollar algunos aspectos relativos al mal llamado "testamento digital"[27]. Al igual que el ordenamiento jurídico español, otros Estados miembros como el italiano[28] o el francés[29], también cuentan con disposiciones para proteger los datos personales tras el fallecimiento incluso antes de la entrada en vigor del RGPD. Este es el caso de Italia y también de España, que ya disponían de protección de la privacidad para las personas fallecidas[30].

Por lo tanto, la investigación que desarrollamos va a tener como normas principales para resolver los problemas jurídicos que se van a plantear el RES, el RGPD y la Ley española de protección de datos personales.

---

25. Sobre la protección de la privacidad tras la muerte *vid*. CÁMARA LAPUENTE, S., "La lesión por medios digitales de la personalidad del fallecido", *Revista de Derecho Civil*, vol. VII, n.º 5, 2020, pp. 117-174.
26. BOE núm. 294, de 6 de diciembre de 2018.
27. Sobre este particular *vid.*, sin carácter exhaustivo, SERRANO COPETE, J., *Los testamentos digital y electrónico: una visión de derecho internacional y comparado*, Tirant lo Blanch, Valencia, 2024.
28. Art 2-terdecies Decreto Legislativo 30 giugno 2003, n. 196 —Codice in materia di protezione dei dati personali—.
29. Art. 63 LOI n.º 2016-1321 du 7 octobre 2016 pour une République numérique, disponible en https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746 (consultado el 2 de mayo de 2025).
30. Art. 2.4 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17, de 19 de enero de 2008).

IV. LA CATEGORIZACIÓN DE LOS BIENES DIGITALES

Uno de los aspectos más complejos que presenta la sucesión de bienes digitales es su categorización para así poder llegar a determinar si esos bienes pueden ser objeto del caudal relicto en una sucesión *mortis causa*. En otras palabras, clasificar la naturaleza del bien digital es una tarea que reviste de cierta complejidad debido a la diversidad de este tipo de bienes y lo relacionado que algunos se encuentran con la identidad de la persona. Además, no se puede perder de vista la importancia del aspecto contractual debido a que la mayoría de esos bienes se crean debido a una relación contractual previa de finado con una empresa que presta servicios en la sociedad de la información.

Un principio importante del que se debe partir es que si el bien digital tiene valor económico se va a poder transmitir por causa de muerte de la misma forma que si de un bien físico se tratara[31]. Este principio ha sido calificado por la doctrina como "principio de equivalencia funcional"[32]. Principio que se puede apoyar en la legislación material sobre sucesiones de ordenamientos jurídicos como el noruego, el inglés, el belga[33] o incluso el español y también en los casos que han tenido que ser resueltos por los tribunales en los últimos años[34]. A la luz de los asuntos resueltos por los tribunales y del derecho material se puede afirmar que al igual que se heredan bienes físicos se podrían heredar bienes digitales. Sin embargo, no es tan sencillo afirmar lo anterior en relación a bienes digitales cuya naturaleza no es estrictamente económica y en los que la privacidad y los derechos de la personalidad, como el honor, la propia imagen, pueden jugar un papel importante, como podría ser una cuenta de email.

De este modo, cada sucesión *mortis causa* en la que existan bienes digitales puede ser muy diferente. Estas sucesiones pueden entrañar dificultades diversas debido a que no existe una visión unánime entre los Estados miembros de qué es un bien digital, de cómo se deben categorizar los mismos ni tampoco cómo debería articularse su transmisión *mortis causa*. Y es que hay

31. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, p. 42.
32. FRAS, M., "Succesion of digital goods. A comparative legal study", *Review of European and Comparative Law*, Volume XLVII, Year 2021, issue 4, p. 79.
33. *Vid.* al respecto FRAS, M., "Succesion of digital goods…", *op. cit.*, p. 78.
34. Uno de los más conocidos, el cual posteriormente desarrollaremos, es el asunto que dio lugar a la sentencia del Tribunal Supremo alemán que dio lugar a una 12 de julio de 2018, un análisis de su recorrido puede estudiarse en FRAS, M., "Succesion of digital goods. A comparative legal study", *Review of European and Comparative Law*, Volume XLVII, Year 2021, issue 4, pp. 70-75.

que tener en cuenta que debido a esa heterogeneidad[35] y diferente naturaleza de los bienes digitales un primer paso sería categorizar dichos bienes en aras de poder determinar si conforme a la Ley que rija la sucesión pueden ser objeto de transmisión *mortis causa*.

Para tal tarea, la doctrina ha diferenciado que los bienes digitales podrían clasificarse en diferentes tipos en atención a si tienen carácter económico o cómo se crean[36]. En atención a si el aspecto más predominante del bien digital es el patrimonial se podría hacer una primera clasificación diferenciando entre:

– *Bienes digitales patrimoniales*. Son aquellos bienes digitales en los que el carácter patrimonial impera. Este podría ser el caso de cuentas bancarias digitales, monederos digitales con criptoactivos, obras de arte como non fungible tokens[37] o la titularidad de derechos de propiedad industrial o intelectual sobre creaciones digitales.

– *Bienes digitales personales*. Estos bienes serían aquellos en los que el aspecto más caracterizador del bien digital es el contenido íntimo, personal o privado de una persona. Estos bienes digitales podrían ser, *ad ex*., mensajes de WhatsApp, cuentas de email o mensajes privados en redes sociales.

---

35. SPANGARO A., *La successione digitale: la permanenza post mortem di aspetti della personalit., Giurisprudenza italiana,* No. 6, 2022, p. 1366.

36. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit*., pp. 42-45.

37. Un "non fungible token" o "token no fungible", también conocido popularmente como NFT, es un activo digital único que no se puede fraccionar, a diferencia de lo que sucede con los "fungible tokens", como es el caso de las criptomonedas (*ad ex*. bitcoins). De este modo, un NFT al no poder ser dividido es irrepetible y está basado en la tecnología de bloques o blockchain. Como consecuencia de esta última tecnología los NFT se pueden almacenar, verificar su autenticidad y demostrar que son únicos, todo ello sería posible gracias a un *smart contract*. En los últimos años, la prensa se ha hecho eco de obras de arte en forma de NFT, algunas de ellas han tenido tal éxito que han sido vendidas por más de 60 millones de euros por famosas casas de subastas como Christie´s. Este fue el caso de la obra "Everydays: The First 5000 Days" del artista Beeple. Vid al respecto, "Las obras de arte más caras que se han vendido como NFT" en Diario Expansión, 15 de febrero de 2022, disponible en https://www.expansion.com/fueradeserie/cultura/2022/02/15/61fae421468aebe9098b45cb.html (consultado el 9 de junio de 2025). Sobre la blockchain *vid*. DE LA MATA RODRÍGUEZ A., "Fundamentos del Blockchain" 2020, disponible en https://blockchainintelligence.es/fundamentos-de-blockchain-por-almudena-de-la-mata/ (consultado el 6 de junio de 2025); LÓPEZ RODRÍGUEZ, A.M., "Ley aplicable a los smart contracts y *lex cryptographia*", *Cuadernos de Derecho Transnacional (CDT)*, Vol. 13, n.º 1, pp. 441-459, en particular, p. 442.

– *Bienes digitales mixtos*. Serían aquellos bienes digitales en los que hay componentes patrimoniales, pero también personales. Es decir, son bienes con naturaleza patrimonial pero también podrían afectar a la privacidad y a la esfera más personal del causante. Este puede ser el caso de la creación de vídeos o publicaciones en redes sociales. Un vídeo o una publicación pueden ser objeto de derechos de autor y que ostente valor patrimonial pero también puede ser contenido que afecte a la esfera privada de una persona y esto implicar que la persona no desee que sus familiares tras su muerte puedan verlo. Del mismo modo, una cuenta de *Apple* o *Gmail* podrían tener también ese carácter mixto.

V. LA DETERMINACIÓN DE LA COMPETENCIA JUDICIAL INTERNACIONAL Y EL DERECHO APLICABLE DE LA SUCESIÓN MORTIS CAUSA DE BIENES DIGITALES

1. EL PUNTO DE PARTIDA

En atención a esta clasificación anterior se podría afirmar que si el bien digital tiene un carácter patrimonial entraría dentro del patrimonio del finado y se regiría por el RES y por sus normas de conflicto aplicables para determinar el Derecho aplicable a la sucesión[38]. En contraposición, siguiendo el mismo razonamiento, si el bien es estrictamente personal quedaría fuera del caudal relicto y podrían entrar en juego otros aspectos no estrictamente sucesorios relacionados con la protección de la privacidad del causante. Sin embargo, la cuestión es qué sucede con esos bienes digitales mixtos o con esos bienes digitales en los que la esfera personal o patrimonial no es tan clara, ¿podrían los herederos ocupar la posición del causante para poder acceder a una cuenta de *Intagram* o *youTube* y seguir "monetizando" contenido de una persona fallecida? La respuesta a esta cuestión estaría relacionada en gran medida con lo dispuesto en los contratos firmados entre el causante y el prestador de servicio digitales que permite el acceso a esas cuentas en plataformas.

De este modo, se deber poner atención en cómo se crea ese bien digital en vida del causante, es decir, qué términos y condiciones se aceptaron por el finado. Estos aspectos serán más que relevantes para poder determinar tanto si los herederos pueden acceder a esas cuentas, qué uso pueden hacer de ese contenido tras la muerte del finado y si el contenido es patrimonial que pueda ser parte del caudal relicto. Es decir, los herederos deben tener presente esos contratos mediante los que sea crea el bien digital para poder determinar cómo impacta en la sucesión *mortis causa*.

38. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, p. 42.

Sobre este particular, la mejor doctrina ha diferenciado que la aproximación a la sucesión de bienes digitales de carácter no estrictamente patrimonial o económico se podría resolver teniendo presente algunas de las siguientes tesis o posiciones doctrinales[39]:

- *Tesis basada en la propiedad*. En base a esta perspectiva, el heredero ocuparía la posición del causante, y, por lo tanto, le sucedería en todas sus relaciones activas y pasivas, incluido los contratos mediante los cuales se crean bienes digitales con independencia de si éstos tienen un carácter más patrimonial o personal. Esta posición se basa en el principio de universalidad de la sucesión y en el principio de equivalencia. Es decir, del mismo modo que se pueden heredar bienes físicos se pueden también heredar bienes digitales con independencia de su naturaleza.

- *Tesis basada en la personalidad*. Esta tesis tiene su eje central en la protección de los derechos de la personalidad y la privacidad del causante. Por lo tanto, en base a esta posición, los herederos podrían heredar algunos bienes digitales de carácter más patrimonial, pero en ningún caso ocupar la posición del causante para poder así heredar cuentas de redes sociales, de email o IDs de *Apple*.

- *Tesis basada en la autonomía de la voluntad*. Esta tesis les otorga un valor importante a los contratos firmados (normalmente condiciones generales de contratación) entre el *de cuius* y las plataformas que prestan servicios digitales. Estas condiciones generales de contratación que firma el usuario normalmente suelen contener cláusulas en las que se precisa qué sucede con la cuenta en causa de muerte. Las soluciones más habituales que ofrecen estas empresas son: 1) La no transferibilidad de la cuenta. Los contratos recogen alguna cláusula en la que se precisa en estos contratos que la cuenta se considere intransferible por lo que los herederos no podrán acceder ni mucho menos ocupar la posición del causante; 2) La no transferibilidad de la cuenta pero con la posibilidad de que el usuario pueda nombrar a un "*heir contact*" o "heredero de contacto" para contactar tras la muerte. Esta persona nombrada *ex profeso* por el causante podrá ser contactada por la empresa de servicios digitales cuando la cuenta lleva inactiva durante un tiempo. También el usuario-causante podrá determinar el contenido al que tendrá acceso esa persona de contacto y qué va a pasar con esa cuenta tras su muerte.

39. SPANGARO A., *La successione digitale: …, op. cit.*, pp. 1368-1370; VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, pp. 43-44.

Desde nuestro punto de vista, las tres tesis centran su atención en aspectos claves para la sucesión digital, esto serían: respeto a la privacidad, autonomía de la voluntad y principio de universalidad. Por eso consideramos que estas tesis no se deberían excluir las unas a las otras sino más bien aplicarse las tres en conjunto en atención al caso concreto.

2. LOS DIFERENTES ESCENARIOS

De este modo, teniendo presente el asunto específico y estas tres posiciones, se podrían diferenciar dos escenarios de partida que podrían estar presentes de forma habitual en una gran mayoría de sucesiones de bienes digitales por causa de muerte. Estos dos escenarios serían:

1) *Escenario enteramente patrimonial*. En este escenario la naturaleza de los bienes digitales que compondrían la sucesión *mortis causa* es patrimonial. Se trataría de un causante que podría tener cuentas de criptoactivos, cuentas en bancos digitales o ser titular de derechos de propiedad industrial o intelectual. En este caso, estos bienes digitales se integrarían en la masa hereditaria en base al principio de universidad y de equivalencia y se podrían heredar como cualquier bien físico más[40]. La determinación del Derecho aplicable en este tipo de asuntos sería del mismo modo que si se tratara de una sucesión *mortis causa* que sólo se compone de bienes analógicos. Por tanto, los artículos aplicables del RES a tener presente serían los arts. 21 y 22. El Derecho aplicable a la sucesión *mortis causa* sería el que determinaría si esos bienes digitales tienen ese carácter patrimonial y si se pueden transferir a los herederos. En principio, todos los contratos firmados por el causante podrían transferirse a sus herederos siempre que no fueran contratos que se extinguen tras la muerte. Así se considera al menos en ordenamientos jurídicos como el español[41] o el italiano[42] en los que se parte de que el heredero sustituye al causante en sus posiciones contractuales como regla general. No obstante, habrá que atender a lo dispuesto por *lex sucessionis*. Un ejemplo práctico nos permitirá poner de manifiesto estos preceptos de forma más clara:

40. *Vid.* al respecto sobre la sucesión de bienes digitales de carácter patrimonial, Pérez Vallejo, A.M.ª /Vivas Tesón, I., *La transmisión mortis causa…, op. cit.,* p. 213.
41. ROSALES DE SALAMANCA RODRÍGUEZ, F., "Testamento digital", en OLIVA LEÓN, R./VALERO BARCELÓ, S.(Coords.), Testamento ¿digital?, Editores Juristas con futuro, 2016, p. 29. Disponible en abierto en https://dialnet.unirioja.es/servlet/libro?codigo=657167 (consultado el 9 de mayo de 2025).
42. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, nota 19, p. 44.

La señora Smith, nacional irlandesa y residente en Marbella desde hace más de una década ha fallecido recientemente en España dejando una masa hereditaria valorada en medio millón de euros. Los bienes que componen el caudal relicto serían de un bien inmueble en Marbella, 100.000 euros que se encuentran en un banco de los que no tienen sucursal, 15.000 euros en una cuenta de *PayPal*, 2 bitcoins y derechos de autor sobre unos vídeos que han tenido mucho éxito y por los que *YouTube* abona una cantidad de dinero cada cierto tiempo a la Sra. Smith. Sus herederos, quieren saber qué Ley regiría esta sucesión *mortis causa* debido a que se compone tanto de bienes digitales como físicos. Para ello hay que tener presente los arts. 21 y 22 del RES. En atención a esta norma hay que determina si la causante eligió el Derecho aplicable a la sucesión conforme a las reglas que establece el RES en su art. 22. En este caso al no existir elección de Ley, el Derecho aplicable se determinaría conforme al art. 21 RES. Este precepto señala que la sucesión se rige en su totalidad por la Ley del Estado en el que el causante tuviera su residencia habitual al momento de fallecer. Es decir, el Derecho español, debido a que la Sra. Smith residía habitualmente en Marbella al momento de su fallecimiento. Es Marbella el lugar en el que la causante se encontraba físicamente en los años previo a su fallecimiento y donde mantenía sus vínculos más estrechos. El Código Civil español es el que determinará cómo se integran esos bienes digitales en la sucesión *mortis causa,* que al tener carácter enteramente patrimonial, se integrarían en el caudal relicto como si se tratara de otros bienes analógicos más.

2) *Escenario patrimonial y personal*. Sucesión de bienes digitales en los que el carácter de los mismos es patrimonial pero también los hay de carácter personal y de naturaleza mixta. En este escenario se tendrá que tener presente la Ley aplicable a la sucesión pero también los contratos firmados entre el causante y los proveedores de servicios digitales[43]. Esto es así debido a que esos contratos de bienes digitales en los que hay la esfera de la persona se ve afectada es necesario analizar si disponen algo esos contratos sobre qué sucede tras la muerte del usuario, y en su defecto, qué dispondría la Ley aplicable a esos contratos. A este particular le dedicaremos el siguiente epígrafe del capítulo.

43. *Ibidem*, p. 44.

3. LA DETERMINACIÓN DEL DERECHO APLICABLE BIENES PERSONALES Y MIXTOS

Partamos de la siguiente situación: el señor Van Dijk de nacionalidad holandesa, con residencia habitual en Alicante fallece en junio de 2025, sus bienes al momento de fallecer serían una cuenta bancaria, títulos valores, dos bienes inmuebles, uno en Ámsterdam y otro en Alicante, una cuenta en la plataforma *OpenSea*, en la que hay 3 NFTS y varias cuentas en Redes Sociales como *Instagram* y *YouTube* de las que recibe dinero de la plataforma debido a que sus últimos años se ha dedicado a crear vídeos y posts sobre automóviles de lujo. Sus hijos quieren heredar cuanto antes y seguir obteniendo rendimiento de las inversiones del causante y de su considerable éxito y rédito en Redes Sociales, pero necesitan acceder a las cuentas y tomar decisiones al respecto. Esto se les presenta más complejo debido a que el causante no dispuso nada sobre su legado digital, tampoco señaló persona encargada ni dejó precisado dónde encontrar claves para poder acceder. De este modo, ante este escenario, la primera cuestión que surge en esta sucesión *mortis causa* transfronteriza es qué Derecho regiría esta sucesión y cómo se integran esos bienes digitales en la misma.

En relación con el primer aspecto, es necesario señalar que el Derecho aplicable se debería determinar en atención a los preceptos del RES citados anteriormente. Es decir, los arts. 21 y 22.

En defecto de elección de Ley válida conforme al art. 22 RES, el Derecho sucesorio español recogido en el Código Civil sería la normativa aplicable debido a que la residencia habitual del causante al momento de fallecer se encontraba en España y esta es la Ley aplicable a la que remite la norma de conflicto del art. 21 RES. Sin embargo, en este asunto que planteamos, el causante era propietario de bienes digitales con carácter patrimonial pero también de bienes digitales de naturaleza personal o mixta. Así, en este caso, aunque el Derecho sucesorio hay que tenerlo presente, también se debe tener el contrato o términos generales de la contratación que el causante firmó[44] para poder acceder a sus cuentas e interactuar en Redes Sociales o en plataformas de *NFTs*. Estos contratos pueden plantear escenarios diferentes en la sucesión *mortis causa* de bienes digitales. Así, es posible diferenciar entre:

1) *Contratos con plataformas que sí incluyen disposiciones relativas a la muerte*. En la actualidad, este escenario es el más habitual debido a que los términos y condiciones de la mayoría de los prestadores de servicios de la información sí precisan qué sucede con la cuenta tras

44. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, nota 19, p. 44.

la muerte del usuario. Un ejemplo de ello es la cuenta de *icloud* de *Apple*. En los términos y condiciones de la empresa de la empresa de Cupertino se puede observar que los contratos de las cuentas de *icloud* son intransferibles, y que, con la muerte del titular, la cuenta y su contenido se acabaría[45]. En este escenario prima la autonomía de la voluntad y la Ley que rige la sucesión permanece en un segundo plano. Los contratos firmados con plataformas en los que se señala de forma expresa que son intransferibles, los herederos no van a poder ocupar la posición del causante y deberán atender a lo que señalan los mismos para poder acceder al contenido. Siguiendo con el ejemplo de *icloud*, en sus condiciones de uso del servicio prevé que el usuario pueda designar un contacto para que tras la muerte ostente determinados derechos concretos sobre la cuenta del causante. Este contacto podría, *ad ex*., descargarse determinado contenido siempre tras la comprobación por parte de *Apple* de que el usuario ha fallecido y de que, esa persona fue designada como contacto tras la muerte[46]. En este escenario se podrían dar situaciones en las que la familia del causante se viera enfrentada a la plataforma y tuvieran que litigar.

2) Contratos *con plataformas que no incluyen disposición alguna en relación al fallecimiento del usuario*. En este escenario la Ley aplicable sería la Ley que rige esos contratos. Si en esa Ley no se señala nada ni se excluye la transferibilidad (que eso va a a ser raro) la sucesión *mortis causa* volvería a entrar en escena y se aplicaría con independencia de que los bienes digitales no ostentaran valor económico[47]. Esto es posible si en el contrato firmado entre el finado y el prestador de servicios digitales no señala nada sobre qué sucede en caso de muerte ni se excluye la transferibilidad del contrato ni tampoco se señala nada en el Derecho aplicable a ese contrato. La transferencia de bienes digitales en este supuesto tan particular sería igual que

45. *Vid.* al respecto, Cláusula IV, letra D, donde se señala lo siguiente: "Except as allowed under Digital Legacy and unless otherwise required by law, you agree that your Account is non-transferable and that any rights to your Apple Account or content within your Account terminate upon your death. Upon receipt of a copy of a death certificate your Account may be terminated and all content within your Account delete".

46. *Vid.* sobre este particular, with Digital Legacy, you can choose to add one or more contacts to access and download certain data in your account after your death. If your designated contacts provide proof of death to Apple and have the required key, they will automatically obtain access to that certain account data and activation lock will be removed from all your devices. Thus, it is your responsibility to keep your Digital Legacy contacts up to date.

47. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, p. 44.

si de bienes analógicos se tratara, salvo que el finado hubiera dispuesto de forma expresa que prohíbe el acceso a sus bienes digitales. En atención al ordenamiento jurídico español, el art. 96.1 letra a) de la Ley española de protección de datos personales precisa que las personas vinculadas con el causante por razones familiares o de hecho, así como sus herederos no podrán acceder a los contenidos del causante ni solicitar su modificación ni eliminación cuando la persona fallecida así lo hubiera manifestado de forma expresa. Esta prohibición manifestada de forma expresa por el causante tiene un límite y es que no puede afectar a al caudal relicto.

En este escenario se pueden dar situaciones en las que los herederos se vean avocados a litigar con el prestador del servicio. Este escenario podría ocurrir cuando en las condiciones y términos del contrato no se prevé nada sobre la transferibilidad de la cuenta en la red social y la familia desea acceder a la misma tras la muerte del usuario, pero el prestador del servicio se niega. Sobre este particular ha habido asuntos que han sido objeto de estudio por la doctrina como el de unos padres que demandaron a *Facebook* en Alemania[48] o el de otros contra *Apple* en Italia[49].

48. El *Bundesgerichtshof* de 12 Julio de 2018 pone fin a una batalla judicial de varios años entre unos padres y la compañía norteamericana *Facebook*. En este asunto se resolvía el litigio entre unos padres alemanes que perdieron a su hija de quince años en un accidente de tranvía. Los padres sospechaban que esa muerte pudo ser consecuencia de que su hija hubiera sufrido acoso y creían que la red social *Facebook* ayudaría a esclarecer lo ocurrido. Sin embargo, *Facebook* se niega a permitir acceso a los padres a la cuenta de su hija, el argumento que esgrime es la seguridad de sus usuarios. En primera instancia, el *Landesgericht* de Berlín en su resolución de 7 de diciembre 2015, dio la razón a los padres y les permitió acceder a la red social. El razonamiento del tribunal se basaba en que tenían derecho a acceder pero no a heredar el contenido existente en la cuenta de la red social. En segunda instancia, el tribunal de apelación, el *Kammergerich* en su sentencia de 31 de mayo de 2017, revoca la decisión de primera instancia y deniega el acceso a los padres a la cuenta de *Facebook* de su hija fallecida en base al secreto en las telecomunicaciones. En particular, el tribunal alemán basándose en la Telekommunikationsgesetz considera que a las cuentas de Facebook también se puede extender el secreto a las telecomunicaciones. El tribunal, en esta segunda instancia, no entra a analizar si una cuenta en una red social puede integrar el caudal relicto y ser parte de la masa hereditaria. Los padres no se resignan ante esa resolución y acuden al Tribunal Supremo alemán. Este resuelve en su sentencia de 12 de julio de 2018 considerando que es posible heredar la cuenta de la hija en *Facebook*, y no sólo su contenido. El Tribunal Supremo alemán basándose en el art. § 1922(1) BGB considera que el acceso y transmisión e incluso posterior uso por parte de los herederos de la cuenta en la red social *Facebook* no vulneraba los derechos de la personalidad de la hija fallecida ni tampoco el secreto de las comunicaciones. Esto permitió que los padres tuvieran no solo acceso al contenido de la cuenta sino que también se les

Por lo tanto, el aspecto clave es estudiar qué señalan esos contratos firmados entre el prestador de servicios digitales y el finado para llegar a determinar la legislación por la que se rigen. Si esos contratos con esos prestadores de servicios digitales no precisan nada o no señalan que la relación se extingue con la muerte, todo quedará regido por el Derecho aplicable a la sucesión[50]. No obstante, la Ley que rige esos contratos es relevante porque puede que el contrato no establezca nada sobre qué sucede tras la muerte del usuario, pero el Derecho que rige esos contratos sí precise que los herederos no pueden suceder al causante en su posición contractual con la plataforma.

4. LOS LITIGIOS DERIVADOS DE LA SUCESIÓN MORTIS CAUSA DE BIENES DIGITALES Y LA DETERMINACIÓN DEL TRIBUNAL COMPETENTE

Una cuestión interesante desde la perspectiva de litigación transfronteriza es qué normas de Derecho internacional privado son las aplicables para determinar el tribunal competente en el caso de una disputa entre herederos y la plataforma prestadora del servicio digital en relación a cuestiones relacionadas con bienes digitales de carácter patrimonial. La doctrina ha considerado que los arts. 4 a 11 RES[51] serían los aplicables y podrían determinar con precisión dónde acudir a litigar[52]. En defecto de elección

considerara herederos de la misma. Para un análisis de este importante asunto *vid*., FRAS, M., "Succesion of digital goods. A comparative legal study*", Review of European and Comparative Law*, Volume XLVII, Year 2021, issue 4, pp. 70-75.

49. Auto del Tribunal de Milán de 9 de febrero de 2021. En este caso unos padres italianos litigaron ante tribunales de Milán contra Apple debido a que querían acceder a la cuenta *en la nube (icloud)* de su hijo menor fallecido en un accidente de tráfico. Tras el accidente, el móvil había quedado destruido y temían que tras tiempo sin actividad, Apple pudiera destruir el contenido de su cuenta. Los padres argumentaron que querían acceder a la cuenta para poder acceder a las fotos y tenerlas de recuerdo. Sin embargo, la empresa californiana se negó debido a que entendía que el Reglamento de protección de datos era inaplicable. Su argumento era que debía protegerse la privacidad y la seguridad de sus clientes resultando de aplicación la Ley estadounidense para las comunicaciones privadas (*Electronic Communications Privacy Act*). El tribunal de Milán consideró que los padres tenían razón y que se debía actuar con prontitud para evitar que se borrara el contenido. Sobre este asunto *vid*., MASPES, I., "Morte digitale e persistenza…", *op. cit*., pp. 1601-1609.
50. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit*., p. 45.
51. CASTELLANOS RUIZ, E., "Sucesión hereditaria.El Reglamento Sucesorio europeo", en CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, pp. 2385-2413.
52. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit*., p. 46.

de foro (art. 7 RES)[53], los tribunales que se tendrían que tener presente por orden jerárquico son:

1.º) Foro de la residencia habitual del causante en el momento de su fallecimiento (art. 4 RES). Un lugar relevante al que acudir a litigar es el de la residencia habitual del causante al momento de su muerte. Aunque no hay un concepto jurídico propiamente definido en el texto del RES sobre qué debe entenderse por residencia habitual, el TJUE sí lo ha ido desarrollando en atención a los asuntos que ha tenido que resolver en estos años[54][55]. En definitiva, una persona física en atención al RES tiene su residencia habitual del Estado miembro cuando del conjunto de circunstancias (en los años de su vida que preceden a su muerte y del momento en el que esta se produce) puede establecerse un vínculo estrecho y estable con un Estado miembro. Ese vínculo lo determinarán especialmente el lugar de su presencia física (teniendo en cuenta su duración y regularidad[56]) y sobre todo en casos de más dudas, su ánimo de permanecer (las condiciones y motivos de esa residencia habitual) también se deberá tener presente. Es un concepto fáctico en el que las circunstancias del caso concreto determinarán en qué Estado reside el causante al momento de su fallecimiento.

2.º) Foro del lugar de situación de los bienes de la herencia (art. 10.1 RES). Un tribunal podrá ser competente en virtud de dónde se encuentren

53. En virtud del art. 7 RES, el causante que haya elegido la Ley aplicable a su sucesión también se puede derivar de ello la elección de foro. Esta elección es limitada y sólo podría implicar la competencia bien de los tribunales del Estado de la nacionalidad del causante al momento de la elección o la de los tribunales del Estado de la nacionalidad del causante al momento de su fallecimiento. Para que este foro pueda operar la elección de Ley debe ser válida en atención al art. 22 RES y además debe existir, bien un acuerdo de litigación entre las partes bien formal o informal de acudir a litigar ante los tribunales del Estado miembro cuya Ley fue elegida por el causante, o bien, el tribunal del Estado del Estado miembro del lugar de la residencia habitual del causante o del lugar de situación de los bienes hereditarios se ha abstenido, a instancia de parte, de conocer del caso porque entiende que los tribunales del Estado miembro del Estado de la ley que fue elegida están mejor situados para conocer. Para un mayor detalle sobre este foro, *vid.* CARRASCOSA GONZÁLEZ, J., El Reglamento sucesorio…, *op. cit.*, pp. 161-169.

54. STJUE de 16 de julio de 2020, C-80/19, *E.E. vs. K.D.E*, ECLI:EU:C:2020:569, apartados 37-40.

55. También los considerandos 23 y 24 del propio texto del Reglamento en materia de sucesiones aunque no define el concepto de residencia habitual ofrece unas consideraciones prácticas útiles sobre la determinación de la residencia habitual.

56. STJUE de 16 de julio de 2020, C-80/19, *E.E. vs. K.D.E*, ECLI:EU:C:2020:569, apartados 38.

sitos los bienes de la herencia y lo será para toda la herencia en su totalidad, siempre que concurran dos requisitos: 1) No concurre ni el foro de la elección de ley (art. 7 RES) ni el foro de la residencia habitual del causante (art. 4)[57]; 2) Algunos bienes de la herencia se encuentran sitos en el Estado cuyos tribunales pueden ostentar competencia judicial internacional. Y además debe concurrir junto con esos dos requisitos un factor *extra* de vinculación que puede ser, bien que el causante ostentara nacionalidad del Estado donde se encuentran los bienes al momento de su fallecimiento o, que el causante hubiera tenido residencia habitual en ese Estado miembro.

3.º) Foro del lugar de situación de los bienes de la herencia (art. 10.2 RES). En el caso de que no concurran ninguno de los foros anteriormente mencionados y existan bienes en un Estado miembro, ese Estado ostentará competencia únicamente para los bienes sitos en su territorio[58].

4.º) Foro de necesidad (art. 11 RES). Este foro puede operar únicamente a favor de un Estado miembro de forma restrictiva y subsidiaria cuando no concurre ninguno de los foros anteriores, la sucesión presenta suficiente conexión con un Estado miembro y además, resulta imposible iniciar un litigio o no puede desarrollarse en un tercer Estado donde sí se presenta el asunto vinculación estrecha.

Sin embargo, estos foros no serían los aplicables en el caso de una litigación transfronteriza cuando la disputa entre los herederos y la familia atañe a bienes digitales con un carácter personal. Es decir, piénsese en el caso de que unos herederos quieren acceder a la cuenta de *Gmail* de su madre fallecida. En el caso de que los bienes digitales no ostenten valor económico, pero sí personal habrá que atender a los instrumentos legales internacionales que permitan determinar la competencia judicial internacional y el Derecho aplicable en los asuntos relativos a la vulneración de los derechos de la personalidad. Especialmente, este escenario de litigación transfronteriza cobrará más fuerza si además hay un contrato entre el prestador de servicios digitales y el causante donde se señala que la cuenta es intransferible. La litigación transfronteriza en estos casos no podría sustentarse en el RES debido a que estos bienes personales intransferibles quedarían fuera del art. 3 del RES[59].

57. STJUE de 7 de abril de 2022, C-645/20, *V A y Z A vs. TP,* ECLI:EU:C:2022:267, apartado 30.
58. CASTELLANOS RUIZ, E., "Sucesión hereditaria. El Reglamento Sucesorio europeo", en CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, p. 2403.
59. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, p. 47.

Así, los herederos y/o familiares del causante deberían tener presente el Reglamento 1215/2012, conocido como Reglamento Bruselas I bis (RBI-bis)[60], para determinar la competencia judicial internacional y las normas de Derecho internacional privado del foro en materia de vulneración de derechos de la personalidad para determinar el Derecho aplicable. Esto es así debido a que el Reglamento europeo en materia de determinación del Derecho aplicable para reclamaciones extracontractuales excluye de su ámbito de aplicación los derechos de la personalidad (art. 2).

Los posibles foros de competencia judicial internacional serían los foros de sumisión expresa (art. 25 RBI-bis) o tácita (art. 26 RBI-bis), el foro del domicilio del demandado (art. 4 RBI-bis) o el foro especial por razón de la materia (art. 7.2 RBI-bis)[61]. En este caso, los familiares podrían acudir a litigar ante los tribunales del Estado miembro donde se han sufrido los daños derivados de la lesión de los derechos de la personalidad, es decir, daño a la intimidad, a la propia imagen o al honor.

En relación al Derecho aplicable, sería de aplicación en el caso de litigar ante tribunales españoles el art. 10.9 del Código Civil español. Este precepto lleva a aplicar la Ley del país donde se ha producido el daño a los derechos de la personalidad[62].

No obstante, antes de iniciar un litigio para poder acceder a cuentas digitales donde el contenido es enteramente personal habría que tener presente tres aspectos:

1) *Vulneración de la privacidad con el acceso a ese contenido*. Sería necesaria valorar a qué tipo de contenido quiere acceder la familia del causante. Si es un contenido íntimo, privado, se podrían encontrar con la negativa por parte de la normativa europea y nacional en materia de protección de datos personales. Desde la perspectiva del ordenamiento jurídico español, hay que tener en cuenta los arts. 3 y 96 de la ya mencionada Ley española de protección de datos personales.

2) *La prohibición expresa del causante*. El causante tiene la facultad de prohibir que sus herederos acceden a sus bienes digitales. Así se

60. Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (versión refundida), DOUE L 351, de 20 de diciembre de 2012.

61. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, pp. 47 y 48.

62. CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. III, Tirant lo Blanch, 2022, p. 4039.

reconoce en la Ley española de protección de datos en su art. 96.1.a). Esta prohibición expresa del causante tiene como límite que dichos bienes digitales afecten al caudal relicto. Así, *ad ex*., por mucho que prohibiera en vida un causante acceder a determinados vídeos o post creados durante su vida, de prácticamente nada le serviría tal prohibición si los mismos son parte del caudal relicto. Esto sucede cuando sobre esos bienes digitales recaen derechos de propiedad intelectual o la plataforma paga por ellos. En este escenario, a pesar de la prohibición, los herederos van a poder acceder y seguir sacando rédito de ese contenido creado por el causante.

3) *El nombramiento de un "heredero de contacto" o "heir contact"*. El causante ha podido nombrar a un familiar o a un amigo, alguien que bien puede o no ser heredero conforme a la Ley aplicable a la sucesión como persona encargada de eliminar o gestionar el contenido las cuentas en las plataformas digitales en las que tiene cuentas abiertas tales como redes sociales, cuentas de correo electrónico o *marketplaces*. Este particular es importante porque esta disposición expresa de nombrar a un "heir contact" limita el acceso a otros herederos o familiares al contenido digital del causante.

El propio contrato firmado entre el causante y el prestador de servicios suele recoger esta figura del "heir contact", pero habrá que tener en cuenta que los derechos nacionales en materia de protección de datos no autorizan a cualquier persona para poder encargarse de esos trámites. Además, conviene no olvidar el derecho sucesorio aplicable al asunto puede no casar del todo bien con el contrato firmado entre el prestador del servicio digital y el causante y las normas de protección de datos[63]. Esta fricción entre normas sucederá como ya hemos señalado cuando esos bienes digitales ostenten un valor económico pero también personal.

Ad ex., la Ley española en materia de protección de datos en su art. 96.1. señala que dichas personas que se pueden encargar serían:

- *"Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información…".*
- *"El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar…".*
- *"En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal…)".*

63. Pérez Vallejo, A.M.ª /Vivas Tesón, I., La transmisión mortis…, *op. cit*., p. 225.

– *"En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado".*

También en otros ordenamientos como en el italiano en base a su normativa interna (art. 2 terdecies del Decreto legislativo 196/2003 modificado por el Real Decreto Legislativo n.º 101/2018)[64], cualquier persona que pueda probar un interés propio o que persiga proteger los intereses del fallecido, con independencia de que sea heredero o familiar, representante o no, pueden ejercer los derechos de los arts. 15 a 22 del RGDP. En el ordenamiento jurídico italiano hay jurisprudencia que muestra como se ha concedido el acceso a las cuentas en plataformas como *icloud*[65].

Otro aspecto que destacar es que esta designación de un "*heir contact*" puede considerarse un mandato *post mortem* en un contexto transnacional[66]. Cuando la persona designada como heredero de contacto acepta ese encargo y en el caso de que un familiar quisiera impugnar esa disposición del causante habría que tener en cuenta las normas de Derecho internacional privado europeo en materia de contratos. Es decir, el Reglamento Bruselas I bis y el Reglamento UE 593/2008, es decir, el Reglamento Roma I[67].

Por lo tanto, para concluir, un ser querido, un familiar que normalmente será heredero quiere, en general, acceder al contenido digital más personal de su familiar fallecido bien para rendirle tributo o bien para poder conocer causas de su deceso cuando las circunstancias no son claras. Desde nuestro punto de vista, además, conviene tener presente si el causante realizó alguna disposición sobre si nombraba a un heredero de contacto o si prohibía el acceso a sus cuentas. Estos aspectos son importantes tenerlos presentes ya que pueden limitar el acceso al contenido digital del causante[68].

---

64. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, p. 47; *Vid*. también, MASPES, I., "Morte digitale e persistenza…", *op. cit.*, p. 1604.
65. *Vid*. al respecto, Tribunal de Bolonia, de 25 de noviembre de 2021 y Tribunal de Roma, 10 de febrero de 2022. Sobre estas sentencias, *vid*., MANIACI, A./ D'ARMINIO MONFORTE, A., "Eredit. digitale" e accesso ai dati personali del defunto, *Diritto di Internet*, No. 3, 2022, pp. 561-573.
66. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, p. 48.
67. Reglamento (CE) n.º 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I), DOUE núm. 117, de 4 de julio de 2008.
68. VARIENGO, I./ RE, J., "Managing managing cross-border…", *op. cit.*, p. 48.

VI. LA SUCESIÓN DE BIENES DIGITALES CREADOS POR EL CAUSANTE

Como se ha puesto de manifiesto anteriormente, no en todo caso, los herederos tienen asegurado que podrán acceder a una cuenta del causante en una plataforma digital y mucho menos ser herederos de la misma. Como se ha estudiado, el contrato firmado entre el finado y la empresa que ofrece ese servicio digital será un elemento clave a tener en cuenta para saber si los herederos podrían ocupar la posición del causante. Así, puede darse la situación de que unos herederos se encuentren sin poder acceder a una red social, por ejemplo, y esto implique que no puedan heredar el contenido creado por su familiar fallecido (posts, vídeos…) sobre el que recaen derechos de propiedad industrial e intelectual y/o derechos económicos como consecuencia de su monetización en la red (por número de visualizaciones, por ejemplo). Esta imposibilidad de acceder y poder gestionar ese contenido va a afectar a los derechos sucesorios. Así, ante este escenario hay doctrina que ha planteado si este escenario podría implicar una vulneración del orden público, llegando a una respuesta afirmativa[69].

La cuestión es que el Derecho aplicable a la sucesión es el que regiría esta transferencia de bienes digitales sobre los que pueden recaer derechos de autor, derechos de propiedad industrial e incluso económicos por la explotación de esos activos[70]. Hay que tener presente que, si sobre esos bienes digitales recaen derechos de autor y el Derecho aplicable a la sucesión es el español, las reglas de transmisión de los derechos económicos derivados de los derechos de autor se rigen por las reglas generales del Código Civil español (arts. 659 y ss.) o el Derecho foral que resultara de aplicación[71]. Es decir, la plataforma de servicios digitales donde se almacena ese contenido no podría negarse (al menos a la luz del Derecho sucesorio español) en base al contrato firmado con el finado a que los herederos pudieran heredar los derechos económicos derivados de los derechos de autor sobre esas creaciones digitales.

Cuestión más compleja es qué sucede con los derechos morales derivados de las obras ubicadas en plataformas digitales tras la muerte de su creador. De nuevo, sería el Derecho aplicable a la sucesión el que determinaría si los derechos morales se podrían heredar pero sin perder de vista también los arts. 15 y 16 *Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y*

69. MARINO, G., *La successione digitale, Osservatorio del diritto civile e commerciale, No. 1,* 2018, pp. 167-204, en particular 182-183.
70. VARIENGO, I./RE, J., "Managing managing cross-border…", *op. cit.*, p. 47.
71. A. M.ª PÉREZ VALLEJO/I. VIVAS TESÓN, *La transmisión mortis…*, p. 158.

armonizando las disposiciones legales vigentes sobre la materia (en adelante, LPI)[72]. En el ordenamiento jurídico español hay posiciones doctrinales enconadas al respecto[73] debido a que se sigue discutiendo si los derechos morales (derecho de paternidad, de integridad de la obra, de modificación…[74]) son derechos de la personalidad, si su carácter es patrimonial o extrapatrimonial, y por lo tanto, y más importante, si se podrían transmitir *mortis causa*. Desde nuestro punto de vista, siguiendo a doctrina civilista referente en estas cuestiones, se puede afirmar que los derechos morales se pueden transmitir *mortis causa*, pero no son derechos patrimoniales ni tampoco personales[75]. De este modo, para el Derecho civil español serían derechos extrapatrimoniales transmisibles *mortis causa* pero de forma especial[76]. Esto implicaría que ese derecho moral que se heredera no pueda ser ejercido del mismo modo que el autor originario. Estos derechos morales al heredarse sufrirían una transformación con el fin de preservar la memoria del autor y la integridad de su obra. Así, con esta transmisión se perseguiría no tanto que el heredero saque provecho o beneficio propio de esos derechos morales sino más bien como vía para preservar la obra y la memoria de su autor[77].

VII. REFLEXIONES FINALES

La actualidad imperante marcada por el hecho de que las personas tengamos una vida real y física pero también otra digital muy activa hizo plantearnos en el título de este trabajo si nuevos escenarios para el Derecho internacional privado se plantean por la sucesión *mortis causa* de los bienes digitales. La realidad es que así es. La sucesión por causa de muerte de los bienes digitales implica problemas legales diferentes a los que planteaban y siguen planteando la sucesión de los bienes analógicos para el Derecho internacional privado. Estos retos legales se acentúan debido a que, como se ha estudiado, en Europa no hay una normativa ni material ni en materia de Derecho internacional privado que ofrezca respuestas ni tampoco jurisprudencia que realice un análisis internacional privatista de los problemas que suscitan estos asuntos.

A nuestro juicio, cuando se plantean sucesiones *mortis causa* transfronterizas compuestas por bienes digitales y bienes que no lo son habría que tener presente tres aspectos:

---

72. BOE núm. 97, de 22 de abril de 1996.
73. A. M.ª PÉREZ VALLEJO/I. VIVAS TESÓN, *La transmisión mortis…*, pp. 153-173.
74. Art. 14 LPI.
75. A. M.ª PÉREZ VALLEJO/I. VIVAS TESÓN, *La transmisión mortis…*, p. 172.
76. *Ibidem*, pp. 172-173.
77. *Idem*, p. 172.

1) *Disposiciones del causante sobre cómo acceder o qué tratamiento dar a sus bienes digitales tras su muerte.* El mejor escenario al que se podrían enfrentar los herederos es aquél en el que el causante ha previsto qué sucede con sus bienes digitales tras su muerte. Estas disposiciones se podrían hacer en un testamento, especialmente aconsejable sería realizarlo ante notario, por la seguridad jurídica que ofrece. En el mismo, conforme a Derecho civil español, se puede hacer disposiciones patrimoniales como extrapatrimoniales y podría ser la vía para prohibir expresamente el acceso a determinado contenido digital del causante o nombrar un "heir contact" que puede tener la forma legal de albacea conforme a nuestro derecho civil que se encargue de destruir contenido digital más personal o permitir acceso al mismo por parte de otros herederos según la última voluntad del causante.

2) *La identificación y categorización del patrimonio digital.* Si el causante no ha señalado ninguna disposición al respecto sobre su patrimonio digital, el primer paso para los herederos será identificar y clasificar esos bienes digitales en atención a si tienen un carácter patrimonial o personal. Uno de los problemas es la dispersión y la variada naturaleza de estos bienes.

3) *La determinación del derecho que rige esa transferencia.* Si los bienes digitales tienen una naturaleza patrimonial, la Ley aplicable a la sucesión determinada conforme a los arts. 21 o 22 RES regirá la transferencia de esos bienes digitales al patrimonio de sus herederos. Sin embargo, en estos casos no es tan sencilla ni clara la sucesión debido a que muchos de esos bienes aunque tienen carácter patrimonial también sobre los mismos existen unos contratos firmados por el causante y el prestador del servicio digital que pueden obstaculizar el acceso a la cuenta, la monetización de su contenido, etc. Así, lo que señalen esos contratos guardará cierta relevancia, aunque la Ley aplicable a la sucesión en estos casos tenga un peso primordial.

Estos contratos a los que nos referimos donde se fijan los términos y servicios para poder crear una cuenta en Dropbox o YouTube son aún más relevantes cuando los bienes digitales tienen una naturaleza más de carácter personal. En ese caso, la *lex sucessionis* es prácticamente irrelevante para dejar paso a las condiciones contractuales que rigen esa relación contractual entre el causante/usuario y el prestador de servicios de la información. Si no se señala nada sobre la transferencia de esos bienes digitales o qué sucede

tras la muerte del causante con esas cuentas, habría que atender al Derecho aplicable a esos contratos. Si no hay previsión alguna por el Derecho aplicable a esos contratos al respecto (que es raro que así sea a día de hoy), será el Derecho aplicable a la sucesión el que determinaría la transferibilidad de esos bienes digitales de carácter personal.

BIBLIOGRAFÍA

CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, pp. 158-164, pp. 2374-2376.

CARRASCOSA GONZÁLEZ, J., El Reglamento sucesorio europeo: análisis crítico, Rapid centro color, Murcia, 2019.

CASTELLANOS RUIZ, E., "Sucesión hereditaria. El Reglamento Sucesorio europeo", en CALVO CARAVACA, A.L./CARRASCOSA GONZÁLEZ, J., *Tratado de Derecho internacional privado*, vol. I, Tirant lo Blanch, 2022, pp. 2374-2376; 2385-2413.

CASTELLANOS RUIZ, M.J., "Competencia internacional en materia de expedición de certificados sucesorios: a propósito de la Sentencia del TJUE 21 junio 2018, Vincent Pierre Oberle, C-20/17", *Cuadernos de Derecho Transnacional (CDT)*, vol. 12, n.º 1, 2020, pp. 473-511.

CÁMARA LAPUENTE, S., "La lesión por medios digitales de la personalidad del fallecido", *Revista de Derecho Civil*, vol. VII, n.º 5, 2020, pp. 117-174.

DAVÌ, A., "Il nuovo diritto internazionale privato delle successioni nell'Unione Europea", *Cuadernos de Derecho Transnacional*, vol. 5, n.º 2, 2013, pp. 5-139.

DE LA MATA RODRÍGUEZ A., "Fundamentos del Blockchain" 2020, disponible en https://blockchainintelligence.es/fundamentos-de-blockchain-por-almudena-de-la-mata/ (consultado el 6 de junio de 2025).

FRAS, M., "Succesion of digital goods. A comparative legal study", *Review of European and Comparative Law*, Volume XLVII, Year 2021, issue 4, pp. 67-81.

LÓPEZ RODRÍGUEZ, A.M., "Ley aplicable a los smart contracts y *lex cryptographia*", Cuadernos de Derecho Transnacional (CDT), Vol. 13, n.º 1, pp. 441-459.

MASPES, I., "Morte digitale e persistenza dei diritti oltre ka vita della persona física" (Nota a ordinanza Tribunale civile Milano sezione I 9 febbraio 2021*), Giurisprudenza italiana*, 2021, fasc. 7, pp. 1601-1609.

MARINO, G., "La successione digitale", Osservatorio del diritto civile e commerciale, No. 1, 2018, pp. 167-204.

MERCHÁN MURILLO, A., "La sucesión digital y el Reglamento sucesorio. Especial referencia al certificado sucesorio europeo: ¿Es posible su tramitación electrónica?", en CAMPUZANO DÍAZ B./DIAGO DIAGO, P. /VÁZQUEZ RODRÍGUEZ M.ª A., De los retos a las oportunidades en el Derecho de familia y sucesiones internacional, Tirant lo Blanch, 2023, pp. 191-201.

MERCHÁN MURILLO, A., "La sucesión digital internacional y el Reglamento sucesorio europeo 650/2012", Anuario Español de Derecho internacional privado, n.º 21, 2021, pp. 327-357.

PÉREZ VALLEJO, A.M.ª /VIVAS TESÓN, I., *La transmisión mortis causa del patrimonio intelectual y digital*, Thomson Reuters Aranzadi, Navarra, 2022, pp. 203-240.

SANTOS MORÓN, M.J., "La denominada 'herencia digital': ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho Transnacional (CDT)*, Vol. 10, n.º 1, 2018, pp. 413-438.

SERRANO COPETE, J., *Los testamentos digital y electrónico: una visión de derecho internacional y comparado*, Tirant lo Blanch, Valencia, 2024.

SPANGARO A., *La successione digitale: la permanenza post mortem di aspetti della personalit.*, *Giurisprudenza italiana,* No. 6, 2022.

VARIENGO, I./ RE, J., "Managing managing cross-border 'digitalsuccession' in the digital era: preliminary remarks on the new challenges for the current legal framework", *EU and comparative law issues and challenge series*, Special issue — Law in the age of modern technologies, Vol. 7 (2023), pp. 37-52.

Capítulo 11

Los datos como bienes digitales transnacionales*

Antonio Merchán Murillo
Prof. Contratado Dr. de Derecho Internacional Privado (acr. a Titular)
Universidad de Cádiz

SUMARIO: I. INTRODUCCIÓN. II. PRINCIPIOS RECTORES EN LA CONTRATACIÓN DIGITAL AUTOMATIZADA. III. LOS DATOS COMO INFRAESTRUCTURA JURÍDICA: DEL FLUJO INFORMACIONAL AL ACTIVO DIGITAL. IV. TITULARIDAD, CONTROL Y APROPIABILIDAD DE LOS DATOS. V. EL DATO EN MOVIMIENTO: CONFLICTOS DE LEYES Y CIRCULACIÓN TRANSNACIONAL. VI. AUTOMATIZACIÓN Y RESPONSABILIDAD: ATRIBUCIÓN DE ACTOS JURÍDICOS EN ENTORNOS ALGORÍTMICOS. VII. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

La transformación digital ha reconfigurado, radicalmente, el modo en que se establecen y ejecutan los contratos, situando a los datos en el centro de todas las transacciones. La automatización de procesos y la integración de nuevas tecnologías han desplazado el énfasis tradicional en la forma y formalidad de los acuerdos, para enfocarse en la gestión, intercambio y protección de la información. Este nuevo paradigma no solo impone retos tecnológicos, sino que también exige una actualización del marco jurídico vigente, adaptándolo a realidades en las que conceptos clásicos, como la equivalencia funcional, la neutralidad tecnológica y la buena fe, adquieren nuevas dimensiones.

* Este trabajo se ha realizado en el marco del Proyecto de Investigación "Hacia una transición digital centrada en la persona en la Unión Europea", TED2021-129307A-I00, financiado por MICIU /AEI/10.13039/501100011033 y por la Unión Europea "NextGenerationEU"/PRTR, de cuyo equipo de investigación es miembro el autor.

En este contexto, en la contratación digital, los datos se convierten en el elemento esencial para la creación, ejecución y verificación de los acuerdos, transformándose en activos de considerable valor económico. La capacidad de diferentes sistemas para comunicarse e intercambiar datos, conocida como interoperabilidad, es fundamental para asegurar que las transacciones se realicen de manera eficiente y confiable. Este proceso de interconexión tecnológica no solo permite un funcionamiento coordinado entre diversas plataformas, sino que también crea un entorno que fomenta la confianza entre los usuarios.

Además, se evidencia un cambio en la manera de entender la seguridad contractual. La antigua idea de certificación, basada en la dependencia de los proveedores de servicios, ha sido sustituida por una visión orientada hacia la fiabilidad, que se sustenta en la capacidad de los sistemas para operar de forma constante y predecible. Esta evolución propicia la creación de un clima de seguridad que, que nos debe llevar a reforzar la protección jurídica de los datos, considerándolos como bienes digitales susceptibles de ser objeto de derechos de propiedad y de valoración mercantil.

En este contexto, extenderemos el análisis a la compleja red de actores que intervienen en la contratación automatizada: desde los desarrolladores y proveedores de datos, hasta los operadores y usuarios finales, para examinar los desafíos que surgen en la asignación de responsabilidades y en la determinación de la legislación aplicable, distinguiendo entre la dimensión personal de los datos, relacionada con la identidad y la privacidad, y su vertiente patrimonial, vinculada a su potencial económico.

Con todo lo anterior, se tratará de poner énfasis en la necesidad de adaptar el derecho a los nuevos entornos digitales, para garantizar un marco seguro y confiable en las transacciones electrónicas, acorde con la creciente complejidad y globalización del mercado automatizado.

II. PRINCIPIOS RECTORES EN LA CONTRATACIÓN DIGITAL AUTOMATIZADA

Lo primero que debemos tener en cuenta son los principios básicos que rigen la digitalización o la electronificación: a) Principio de equivalencia funcional: constituye el núcleo sobre el que gravita el reconocimiento jurídico de los actos realizados en el comercio electrónico. Sin su aplicación, carecería de eficacia, por lo que se parte de la premisa de que los actos jurídicos electrónicos tienen la misma validez funcional que los escritos; b) Principio

de inalterabilidad del derecho preexistente: todas aquellas reglas dirigidas a la regulación del comercio electrónico no supongan una modificación sustancial del Derecho existente. No obstante este hecho no debe impedir que las normas deban ser interpretadas y adaptadas; c) Principio de neutralidad tecnológica: las nuevas normas que rigen el comercio electrónico abarquen con sus reglas no sólo la tecnología existente sino también toda tecnología futura sin que haya necesidad de modificar estas normas; d) Principio de la buena fe: principio que encuentra su justificación en la idea de que la ignorancia, ante la renovación tecnológica, genera desconfianza; e) Libertad contractual mantenida en el nuevo contexto electrónico: autonomía de la voluntad.

Con relación a este principio se ha observado un cambio de terminología en las normas pasando de seguridad a fiabilidad: a) El término utilizado antes era certificación; es decir, seguridad: induce dependencia, en relación con el origen o la conexión. Ahora, el primero espera una buena conducta. Esto nos va a llevar a problemas de prueba (por ejemplo, la probatio diabólica, en la propuesta de Directiva sobre responsabilidad de los sistemas de IA); b) La fiabilidad como medio nos lleva a una probabilidad de buen funcionamiento. Lo que nos sitúa en la confianza. Desde el punto de vista de la transacción, cuando hablamos de fiabilidad, nos referimos a que un dispositivo trabaje correctamente durante un tiempo y en las condiciones en que se encuentre el servicio, de manera que cuando se realice una transacción, deberá considerarse los posibles riesgos. Por consiguiente, identificamos la fiabilidad como un conocimiento del estado del sistema; c) La fiabilidad nos lleva a la confianza: Se pretende atraer la atención del usuario, creando un clima de confianza en un entorno determinado. De esta forma, se quiere dar a entender como un proveedor de servicios, con sus acciones y sus caracteres, va a conseguir, de Internet, un universo más o menos confiable para las personas.

Junto a los anteriores debe advertirse una estructura propia común a todas las transacciones. Son identificables los siguientes elementos, que pueden ser agrupados en dos apartados: a) Elementos objetivos: que no necesariamente son materiales. Estos elementos son: 1) El mensaje de datos; 2) La norma técnica de estructuración; 3) La firma electrónica; 4) Los sistemas de información; 5) Las redes de transmisión de datos; b) Elementos subjetivos: se comprenden en el mismo los distintos sujetos destinatarios de los mandatos y privilegios legales, así como de los derechos y obligaciones contractualmente adquiridos en el marco jurídico del comercio electrónico. Estos son: 1) El iniciador o firmante del mensaje de datos; 2)

El destinatario del mensaje de datos; 3) Los intermediarios y proveedores de servicios de certificación de firma electrónica o autoridad de certificación. Con lo comentado, se puede realizar una tarea de determinación y definición de cada uno de los elementos principales involucrados en la transacción electrónica, a la vez que se podrían tratar los múltiples problemas derivados de la dificultad de aplicar los diferentes conceptos y las categorías jurídicas.

Todo lo anterior no tiene sentido sin un marco de interoperabilidad: ¿Por qué? Se trata de que sistemas o componentes de *software* para intercambiar y utilizar información entre sí, de manera eficiente y sin problemas. En el ámbito de la tecnología de la información, la interoperabilidad es crucial para garantizar que diferentes sistemas, aplicaciones y dispositivos puedan trabajar juntos de manera armoniosa: a) Organizativos: en los procesos de negocio y estructuras internas (por ejemplo, que actores participan y por tanto van a ser sujetos responsables. Por ese motivo, el ámbito personal de las normas es tan importante); b) Semánticos: los datos comparten el mismo significado (por eso las definiciones son tan importantes: para garantizar no un buen nivel de comunicación sino de interpretación); c) Técnicos: conexión de sistemas sean eficientes sin fallos en materia de ciberseguridad (por ejemplo, intercambio de datos); d) Jurídicos: las normas deben ser neutrales tecnológicamente.

En este contexto, puede observarse que la interoperabilidad no es plena; pues, si bien en todas las normas se aprecia que la base está en los datos, su definición no aparece en ningún lugar, los personales están claro, pero ¿y los no personales?… Donde queda la necesidad de reforzar el control sobre los datos propios: propiedad de los datos.

III. LOS DATOS COMO INFRAESTRUCTURA JURÍDICA: DEL FLUJO INFORMACIONAL AL ACTIVO DIGITAL

Dentro de los contratos automatizados pueden encontrarse los contratos de suministros de datos o procesamiento de datos, porque sin los datos no se puede hacer la programación de la automatización del propio contrato[1]. Es más, puede afirmarse que algunas plataformas en línea establecen un mercado de datos o son operadas por intermediarios de datos y, con ello, puede decirse que el contrato entre el operador de la plataforma de datos y el usuario de la plataforma puede calificarse generalmente como un contrato

1. FERRO, E., "Digital assets rights management through smart legal contracts and smart contracts", *Blockchain: Research and Applications*, junio, 2023, págs. 23 a 45.

de procesamiento de datos[2]. Por supuesto, debe tenerse en cuenta que no hablamos de datos personales, sino de su vertiente patrimonial, datos no personales con un determinado valor económico, tal y como se ha defendido en otros estudios[3].

Puede apreciar como el auge de la digitalización está en la creciente internacionalización porque las personas descritas anteriormente, y por tanto los datos también, difícilmente van a estar en un mismo estado y, en algunos casos, nos encontramos además con sistemas automatizados. En este contexto, desde el Grupo de Trabajo IV de UNCITRAL se ha referido a que las cuestiones relacionadas con los datos "no constituyen un contrato de compraventa y que los datos pueden describirse como mercaderías"[4]. Ahora bien, si bien desde UNCITRAL se habla de datos como información, en nuestra opinión no es así.

Para asentarnos defender nuestra idea debemos asentarnos en el derecho de propiedad de los datos, donde cabría preguntarse, ¿qué tengo para usted? ¿un dato o una información? Los datos y la información son dos conceptos distintos, por qué sin información no hay dato y la información no se puede proteger. Por tanto, sí te doy un dato, lo puedes proteger en internet, sí te doy una información, no se me puede proteger, ya que la información fluye por internet, pero el dato si se piensa bien, permanece y da una verdadera tenencia y, con ello, un verdadero conocimiento sobre algo, entre otras cosas porque puede ser objeto de prueba[5].

Consideraciones al respecto se ha dado a nivel internacional, puede verse si observamos la Sentencia dictada en el caso *Your Response Ltd. v. Datateam Business Media Ltd.*[6], en la Decisiones del Tribunal de Apelaciones de Ingla-

---

2. DIXIT, A., "Towards user-centered and legally relevant smart-contract development: A systematic literature review", *Journal of Industrial Information Integration*, Vol. 26, marzo, 2022, págs. 2 a 45; PINHO, D., "What about the usability in low-code platforms? A systematic literature review", *Journal of Computer Languages*, Vol. 74, enero 2023, págs. 65 a 101.
3. MERCHAN MURILLO, A., "Sucesión digital internacional y el Reglamento sucesorio europeo 650/2012", *Anuario Español de Derecho Internacional Privado*, ISSN 1578-3138, N.º 21, 2020, págs. 327-357.
4. UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: propuesta de labor futura en el ámbito de las operaciones de datos*, Nueva York, 27 de junio a 15 de julio de 2022, pág. 4.
5. UNCTAD, *Informe sobre la Economía Digital 2019: Creación y captura de valor: repercusiones para los países en desarrollo*, Ginebra, 2019, pág. 32.
6. [2014] WLR(D) 131, [2014] 4 All ER 928, [2014] EWCA Civ 281. Disponible en https://www.bailii.org/ew/cases/EWCA/Civ/2014/281.html

terra y Gales (División Civil), en Inglaterra, donde se indica que una base de datos electrónica es un tipo de propiedad intangible. Una base de datos electrónica consta de información estructurada. Aunque la información situada dentro de ésta puede dar lugar a derechos de propiedad intelectual, la ley se ha mostrado renuente a tratar la información en sí misma como propiedad, con relación a los datos. Cuando se crea y registra la información, existen claras distinciones entre la información misma, el medio físico en el que se registra la información y los derechos a los que da lugar la información. Mientras que el medio físico se trata como propiedad, en relación la información electronificada en sí nunca lo ha sido. En este contexto, el Tribunal admitió que había argumentos sólidos a favor del reconocimiento de los datos, como objetos incorporales, como una nueva categoría de bienes, aunque añadió que para introducir esa innovación jurídica sería necesario que interviniera el Parlamento.

En el Estado de Nueva York, el Tribunal de Apelación, se ha aceptado que la acción reivindicatoria se extienda a los objetos incorporales, por ejemplo, en la Sentencia dictada en el caso *Thyroff v. Nationwide Mutual Insurance Co.*[7], donde el Tribunal sostuvo que una acción reivindicatoria entablada al amparo de la legislación de dicho Estado abarcaba los documentos electrónicos almacenados en un ordenador. En este caso, los documentos comprendían información de clientes e información personal almacenada en el sistema informático de un mandante al que un mandatario podía acceder a través de un ordenador con licencia. No obstante, el tribunal advirtió que no había analizado si alguna de las otras e innumerables formas de información virtual, en relación con los datos, debían ser protegidas por las normas de la responsabilidad civil, ya sea contractual o extracontractual.

En la UE, parte de la doctrina jurídica ha entendido que el TJUE en su Sentencia de 3 de julio de 2012, en el asunto C-128/11, UsedSoft GmbH contra Oracle International Corp.[8], abrió la puerta a un debate sobre la propiedad de los objetos incorporales. En ese asunto, el tribunal sostuvo que la distribución comercial de programas informáticos mediante descarga de Internet podía constituir una venta a los efectos de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador. Para llegar a esa conclusión, el tribunal consideró que, según una definición comúnmente aceptada, la "venta" era un contrato mediante el que "una persona transfiere a otra, a

7. Disponible en: https://www.law.cornell.edu/nyctap/I07_0029.htm
8. STJUE de 3 de julio de 2012, UsedSoft GmbH vs Oracle International Corp. C-128/11, ECLI:EU:C:2012:407

cambio del pago de un precio, los derechos de propiedad de un bien corporal o incorporal que le pertenece" y, por consiguiente, consideró que una "operación comercial que da lugar al agotamiento del derecho de distribución relativo a una copia de un programa de ordenador implica que se ha transferido el derecho de propiedad de esa copia" (apartados 44 y 45 de la Sentencia).

En este contexto, defendiendo que los datos pueden ser objeto de propiedad[9] podría establecerse una definición de lo que es un dato, que en nuestra opinión, desde un punto de vista amplio, y, por tanto, como punto de partida útil, en términos de uso, hablamos de aquellos que incluyen la salida de dispositivos analógicos o datos en formato digital, manipulados, almacenados o comunicados por cualquier dispositivo hecho por el hombre, ordenador o sistema informático o transmitidos a través de un sistema de comunicación, que tiene el potencial suficiente para ser gestionado vía internet y por tanto crear un relato fáctico probable y fiable. La característica más destacada va a ser la interposición/mediación de la maquina y el sujeto con los datos, volviéndose inteligible mediante el uso de hardware y *software*, que crean un "el documento" que está en alguna "parte", en formato archivo, y que no existe independientemente del proceso que lo recrea cada vez que un usuario lo abre en su ordenador.

Dicho lo anterior, en internet tienen los datos su entorno y los diferentes estados de los datos y, en nuestra opinión, también podemos identificar los tipos o las clases de datos, partiendo de: a) datos en reposo o almacenamiento; b) Datos en movimiento o de comunicación o contenido; c) Datos en uso o procesados. Además, se pueden observar datos que son relevantes para el cifrado, que incluyen los metadatos, y que son cualquier dato informático relativo a una comunicación por medio de un sistema electrónico. Estos metadatos los podemos clasificar en tres tipos principales: a) descriptivos, que brindan información descriptiva sobre un documento en particular; b) estructurales, que describen la identificación de archivos o la información de codificación de archivos; c) administrativos, que brindan información para ayudar en la administración del documento o recurso[10].

Lo descrito anteriormente, nos debe llevar a identificar a la diversa gama de actores, que están ubicados, por la propia naturaleza de internet, en

9. MASON, S., *Electronic Evidence*, University of London Press, Londres, 2021, p. 167.
10. SCHMIDT-KESSEN, M. J., "Machines that make and keep promises — Lessons for contract automation from algorithmic trading on financial markets", *Computer Law & Security Review*, Vol. 46, Septiembre 2022, págs. 206 a 265.

diferentes Estados, en relación con los datos. Esos diferentes actores son, entre otros[11]:

a) El generador de los datos, una máquina o un sensor, así como los datos que se generan a partir de otros datos. Aquí podemos situar a los nodos

b) El programador de los datos y del sistema

c) El sujeto de los datos o persona a quien se refieren los datos.

d) El proveedor de los datos o persona que suministra los datos, incluida la persona que proporciona los datos que se ponen en común en una plataforma en línea.

e) El receptor de los datos o la persona que recibe los datos, incluida la persona que accede a los datos que se ponen en común en una plataforma en línea.

f) El procesador de los datos o la persona que procesa los datos, independientemente de que los genere o los reciba.

g) El operador de la plataforma de datos o persona que aloja los datos en una plataforma en línea.

Conforme a lo anterior, y desde nuestro punto de vista, parece obvio que los bienes digitales deberían gozar de la protección que confieren las normas del derecho de los bienes. Tienen todas las características de los bienes, y las dificultades conceptuales parecen derivarse principalmente de los orígenes históricos de nuestro derecho de los bienes corporales. Hay una diferencia real entre los bienes digitales y la información registrada en ellos. Esos registros permanentes de información, como datos, pueden ser objeto de posesión o disposición indebida cuando adoptan una forma física, y sería arbitrario basar las normas jurídicas en la forma del soporte, especialmente hoy en día, en que los soportes digitales han asumido un papel omnipresente en la vida moderna.

Ante el contexto manifestado, debe profundizarse en el tráfico jurídico informático. Por ello, si partimos de la validez del Derecho preexistente y el principio de equivalencia funcional, no partimos de cero, ya que el derecho existente sirve para ser adaptado al derecho actual y que el mundo real sirve para adaptar al mundo virtual. Con ello, nos encontramos con que el derecho civil ofrece protección en caso de posesión o disposición indebida

11. UNCITRAL: *Cuestiones jurídicas relacionadas con la economía digital: las operaciones de datos*, Nueva York, 6 a 17 de julio de 2020, pág. 3.

del bien corporal que contiene los bienes digitales; cuando la información registrada en el bien digital se obtiene quebrantando el deber de confidencialidad o infringiendo las normas sobre privacidad; o cuando el bien digital, el dato, está sujeto a un contrato. De esta forma, los datos pueden tener un inmenso valor comercial en el mundo moderno, lo que significa que existe una importante razón económica para garantizar que la ley los proteja como bienes. En cualquier caso, lo que hemos indicado es relevante, poque en los contratos automatizados pueden encontrarse insertos contratos de suministros de datos o procesamiento de datos, lo que nos lleva ahora a la determinación de la Ley aplicable en caso de responsabilidad.

IV. TITULARIDAD, CONTROL Y APROPIABILIDAD DE LOS DATOS

Los datos se nutren de la nube que es donde ubicamos el big data, la IA, Blockchain, IoT, etc., que están marcado el comienzo de una gran revolución, de carácter transfronterizo, en la que surgen cuestiones realmente relevantes rodeadas de problemas legales. Uno de los problemas es la propiedad de los datos personales. Debemos explorar los límites conceptuales de la propiedad de datos para proceder a los debates sobre la propiedad de datos no personales. Teniendo presente que los datos, sean personales o no, se van a reconocer, como trataremos de demostrar más adelante, como activos económicos clave. Por ello, evitar preguntas sobre su propiedad es, por tanto, retrasar la protección de los usuarios.

Dicho lo anterior, partimos del artículo 4,1 del Reglamento 2016/679, 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 (RGPD), que define los "datos personales" como "toda información sobre una persona física identificada o identificable". Esta definición debemos ponerla en conexión con el considerando 68 que infiere la necesidad de reforzar el control sobre los datos propios de una persona, cuando el tratamiento de los datos personales se efectúe por medios automatizados. Con esto, parece referirse la propiedad de los datos, por parte de los interesados. No obstante, los datos personales aparecen en la definición del Reglamento como "información", en este caso, información personal, relacionada con una persona física[12], al igual que nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de

12. PRINS, J.E.J., "The propertization of personal data and identities", *E.J.C.L.*, núm. 8, 2004, pp. 3-25.

Datos Personales y garantía de los derechos digitales (LOPDyDD). Ahora bien, debe observarse que existe una distinción conceptual clara entre los datos y la información, que tiene implicaciones cruciales para determinar la propiedad de los datos[13].

Los datos y la información son dos conceptos distintos[14], por razones obvias, no hay información sin datos; es decir, no debemos comprender la información como cualquier forma transmitir datos, ni la forma de tratar los datos como un activo del que se puede extraer información valiosa de futuro.

De esta forma, puede verse como el RGPD define los datos personales a la inversa, puesto que los datos son la fuente de información[15]. De esta forma, el choque entre la privacidad y la propiedad defendida parece un problema en que no se sabe bien cuál debe ser el primero en solucionarse; pues, si hablamos de que lo importante es la información, todo nos va a llevar *a priori*zar la personal, pero si nos centramos en la propiedad todo conduce a los datos, en su conjunto y debe ser objeto de análisis detallado, puesto que la información no puede ser objeto de propiedad.

El motivo está en que el debate europeo se centró sobre la protección de la privacidad; es decir, desde una perspectiva de los derechos humanos, no desde una perspectiva comercial, que podría conllevar el concepto de propiedad[16]. Ahora bien, este argumento también podría funcionar al revés, en un sentido puro, la idea de los derechos humanos tiene que ver con el empoderamiento y, por ello, podría argumentarse que negarle a cualquier individuo un derecho de propiedad de sus datos y así su privacidad viola sus derechos fundamentales.

En cualquier caso, va a resultar esencial, para determinar la propiedad de los datos conocer: quién recopila la información, quién la analiza, quién la difunde y a quién, la naturaleza de la información, las relaciones entre las distintas partes, e incluso mayores circunstancias institucionales y sociales.

Lo anterior, nos lleva al estudio del objeto de la sucesión digital. Concretamente, por un lado, se pretende distinguir entre distinguir entre la

13. GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la era de las big data y de la computación ubicua*, Dykinson, Madrid, 2016, p. 106.
14. AZIZ, A.; TELANG, R., "What Is a Digital Cookie Worth?", *SSRN*, marzo, 2016, pp. 3-37.
15. JANEČEK, V., "Ownership of personal data in the Internet of Things", *Computer Law & Security Review*, núm. 34, 2018, pp. 1039-1052.
16. FOSCH VILLARONGA, E.; KIESEBERG, P. ; LI, T., "Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten", *Computer Law & Security Review,* vol. 34, núm. 2, 2018, pp. 304-313.

identidad digital (el sujeto)[17] y el patrimonio digital (el objeto), surgiendo aquí la necesidad de realizar una diferenciación, que en nuestra opinión, se antoja fundamental entre: los datos personales que te identifican o te hacen identificable y la posible mercantilización de los datos (que podrían ser datos no personales), puesto que a menudo se habla de "contenidos digitales" ("los datos producidos y suministrados en formato digital", según el artículo 2,1 de la Directiva 2019/770, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales), en términos generales, pero realmente puede que estemos hablando de nuestros datos. Por este motivo, es posible detectar:

a) Una vertiente personal: datos personales, intimidad, etc. Que en suma van a constituir la identidad digital de una persona.

b) Una vertiente patrimonial: activos o bienes digitales, que pueden tener un alto valor de mercado, por ejemplo, los datos no personales. En este apartado también podría incluirse, en algún caso, lo anterior siempre que los datos de los usuarios sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (artículo 5,1, c RGPD).

Dicho de otro modo, hablamos de: identidad digital (el sujeto, en tanto que los datos personales te identifican o te hacen identificable) y lo que podría considerarse como patrimonio digital (el objeto, la posible mercantilización de los datos)[18], puesto que a menudo se habla de "contenidos digitales", en términos generales, cuando realmente puede que estemos hablando de nuestros datos. Motivo por el que es posible detectar una vertiente personal (datos personales, intimidad e identidad digital) y una vertiente patrimonial (todo tipo de "activos digitales" pueda tener un alto valor de mercado, en el que podrían incluirse en algún caso lo anterior y, además, los datos no personales. Todos ellos como activos).

En definitiva, podríamos hablar de un entorno intrínsicamente personal, es decir datos que son y pertenecen únicamente a la esfera privada de la persona, y un entorno que no es intrínsicamente personal[19]. Los primeros

17. MADRID PARRA, A., "La identificación electrónica", *Revista de la Contratación Electrónica*, núm. 15, 2001, pp. 5-61.

18. CÁMARA LAPUENTE, S., *La sucesión mortis causa en el patrimonio digital: una aproximación, conferencia dictada en el colegio notarial de Madrid*, salón académico, el 24 de enero de 2019, puede consultarse en http://www.elnotario.es/index.php/academia-matritense-del-notariado/9279-la-sucesion-mortis-causa-en-el-patrimonio-digital-una-aproximacion

19. JANEČEK, V., "Ownership of personal data in the Internet of Things", *Computer Law & Security Review*, núm. 34, 2018, págs. 1039-1052.

son los que estaría o serían objeto de protección por la propia normativa de protección de datos y los segundo son los que serían objetos del derecho a la propiedad de los datos.

En relación con la propiedad de los datos deben observarse dos perspectivas bajo las cuales se puede analizar la propiedad y mezclarlas puede generar confusión. Por un lado, encontramos la propiedad "de" la nube, compuesta de un hardware y un *software*[20], que constituyen los activos comerciales del proveedor del servicio; por otro lado, la propiedad "en" la nube, ante la necesidad de garantizar la protección de los datos de los usuarios, lo que podrían denominarse bienes o activos digitales. En este contexto, surgen cuestiones de propiedad intelectual planteadas a raíz de modificaciones de datos de los clientes y derechos de propiedad sobre los datos procesados en la nube, por ejemplo, metadatos[21].

De esta forma, como decimos, la propiedad "de" la nube se estructura básicamente en dos componentes: hardware y *software*, los cuales constituyen los activos comerciales del proveedor del servicio. El primero consiste en un conjunto de bienes materiales, sujetos a las reglas de propiedad comunes, y cuya circulación depende de las leyes estatales. La del *software* es una situación más complicada, debido a que está sujeto al complejo marco de las normas de propiedad intelectual. Por otro lado, la propiedad "en" la nube, que consiste en la necesidad definida, a nivel global, de garantizar que los usuarios retengan el control sobre sus propios datos. Estos datos, por ejemplo, pueden ser escritos u otras obras de arte (incluidas fotografías que no pueden considerarse datos personales), notas, documentos utilizados para nuestro trabajo, documentos privados, copias de seguridad, materiales electrónicos comprados, como libros, música o películas, *software*, etc.[22]. En esta segunda cuestión nos situaremos.

En este contexto debe tenerse en cuenta que, en nuestro derecho, si nos situamos en el artículo art. 348 CC "la propiedad es el derecho de gozar y disponer de una cosa, sin más limitaciones que las establecidas en las leyes.

---

20. CUERVA DE CAÑAS, J. A., "La propiedad intelectual en el mundo digital", en *Sociedad Digital y Derecho* (Tomás de la Quadra-Salcedo y Fernández del Castillo (Dir.), José Luis Piñar Mañas (aut.), Ministerio de Industria, Comercio y Turismo, 2018, págs. 719-740.
21. PABÓN CADAVID, J., "Protección legal a los metadatos y la gestión digital de los derechos de autor", *Ius et Praxis*, Vol. 26, núm. 1, 2020, págs. 57-76; DE MIGUEL ASENSIO, P. A., "Mercado único digital y propiedad intelectual: las Directivas 2019/789 y 2019/790", *La Ley Unión Europea,* número 71, 2019, págs. 21 a 56.
22. CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J., *Derecho Internacional Privado*, vol. II, 18.ª Ed., Comares, Granada, 2018, pág. 1363.

El propietario tiene acción contra el tenedor y el poseedor de la cosa para reivindicarla". Como puede observarse en, un sentido estricto, el término describe una relación entre una persona y una cosa, y no la cosa en sí, por lo que puede decirse que nos estamos refiriendo a los objetos que pueden ser derechos de propiedad. Asimismo, apreciable es que en nuestro ordenamiento jurídico que la propiedad puede dividirse en bienes inmuebles y bienes muebles y que los derechos que se reconocen derechos relacionados con la posesión de la cosa y derechos relacionados con "cosas en acción" (derechos o reclamaciones legales exigibles por acción).

Por lo anterior, en nuestra opinión, por equivalencia funcional debe tenerse encuentra que hablamos de un bien digital que es definible, identificable por terceros, capaz por su naturaleza de ser adquiridos por terceros, tiene carácter permanente y estable, valor. Por ello, pueden identificarse datos representados en un medio electrónico, incluyendo en forma de código informático, señales electrónicas, digitales o analógicas, que conllevan representación de un conjunto de datos que pueden referirse a derechos sobre la cosa con el fin de poseerla, venderla, prestarla, usarla y beneficiarse de ella. Tradicionalmente, "debe ser definible, identificable por terceros, capaz por su naturaleza de ser asumido por terceros y tener algún grado de permanencia o estabilidad". Por ello, la lista de categorías de propiedad es "exhaustiva, pero ampliable".

V. EL DATO EN MOVIMIENTO: CONFLICTOS DE LEYES Y CIRCULACIÓN TRANSNACIONAL

Para hablar de esta cuestión, partimos del caso *B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l)*[23], donde la decisión adoptada por un Tribunal de Singapur tiene implicaciones en relación con los contratos automatizados, la IA y si las criptomonedas son consideradas como propiedad. Nosotros solo nos vamos a centrar en las primeras cuestiones, con relación a la naturaleza automatizada de la Plataforma que, según el Tribunal, podría dar lugar a transacciones que tengan un efecto contractual legalmente vinculante y cómo se determina el conocimiento, a los efectos de establecer un error cuando los contratos se celebran de forma automatizada por ordenador y no a través de la toma de decisiones humana[24].

23. Caso B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l) 3. Disponible en: https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/quoine-pte-ltd-v-b2c2-ltd.pdf

24. D. KIAT BOON SENG, "Quoine Pte Ltd v B2C2 Ltd: A Commentary", *China-Singapore "One Belt One Road" International Business Cases Digest Part* 1. Disponible en: SSRN:

Conforme a lo anterior, el Tribunal señaló que "toda la información necesaria para la formación del contrato electrónico ha sido preprogramada, según estrictos parámetros establecidos por la empresa, en el *software* informático de la SSP". Por lo tanto, los datos relevantes se procesan automáticamente por medios electrónicos a través del *software* de un ordenador y las transacciones se ejecutan automáticamente dentro de los parámetros especificados predeterminados en el programa. Una vez realizado, usando su ordenador y accediendo al *software* SSP, se introducen los datos necesarios, la oferta es generada automáticamente por el propio programa sin más intervención humana y, una vez que se han tomado los pasos requeridos por el programa para una aceptación de la oferta, la aceptación es procesada automáticamente por el propio programa, de nuevo sin intervención humana adicional[25]. De esta forma, los usuarios que tenían acceso al *software* SSP, creado por una empresa programadora, podían usar el programa con el fin de formalizar el contrato, con la otra parte del contrato, comprometiéndose a que, si se seguían las instrucciones previas; es decir, conforme a los procedimientos programados, estarían obligados por el resultado generado automáticamente, incluso si la parte destinataria o un tercero, que podría identificarse como los usuarios finales, a quienes van destinados lo productos finales, que son terceros en discordia, desconocían temporalmente ese resultado. El proceso podría describirse en una empresa fábricas, otra las compra a través de una plataforma programada por un tercero quizá por encargo, esta misma la distribuye para un usuario final u otra y yo, usuario final utilizo el producto).

De esta forma, puede observarse que, en el presente caso, una parte ofrece el *software* SSP como el medio automático para la formación del contrato. Una vez que la otra parte ha metido los datos necesarios en el programa informático, no se necesita más intervención humana para la formación de un contrato vinculante entre una y otra parte. Ahora bien, el producto resultante puede llegar defectuoso al usuario final si hay un error en el sistema. Estos fallos pueden deberse a errores en el procesamiento de datos, falta de acceso a fuentes externas o ausencia de salvaguardas en la programación para evitar operaciones incorrectas.

Como ya hemos comentado, hablamos de programas que operan cuando se les llama a hacerlo de manera preestablecida. Son meras máquinas

---

https://ssrn.com/abstract=3960007 or http://dx.doi.org/10.2139/ssrn.3960007

25. WONGPARTNERSHIP LLP, "Singapore Court of Appeal Clarifies Application of Unilateral Mistake in Algorithmic Trading", *Casewatch*, Julio, 2020. Disponible es: https://www.wongpartnership. com/upload/medias/KnowledgeInsight/document/15268/20200702_CaseWatch_SingaporeCourtofAppealClarifiesApplicationofUnilateralMistakeinAlgorithmicTrading.pdf

que llevan a cabo acciones que en otra época habrían sido realizadas por un humano debidamente capacitado. No son diferentes, por ejemplo, a un robot de cocina que me puede ayudar a hacer un gazpacho Hablamos de máquinas que operan como han sido programadas una vez activadas. De esta forma, como dice la Sentencia "cuando es relevante determinar cuál era la intención o el conocimiento subyacente al modo de operación de una máquina en particular, es lógico tener en cuenta el conocimiento o la intención del operador o controlador de la máquina". En el caso del robot de cocina, nosotros como personas físicas seremos quienes coloquemos los ingredientes y la pune en funcionamiento. Su conocimiento o intención será contemporáneo a la operación que va a hacer la máquina, en nuestro ejemplo el gazpacho, "pero en el caso de los robots o el *software* de los ordenadores, esto no será así. El conocimiento o la intención no pertenecen a quien enciende el sistema, sino al programador responsable de su funcionamiento". Esto necesariamente se habrá hecho en una fecha anterior a la fecha en la que el *software* del ordenador o del robot llevaron a cabo los actos en cuestión. En este sentido, rechazo el argumento de la parte demandada de que el único conocimiento relevante es el conocimiento al momento de contratar. Sin embargo, se muestra de acuerdo con el demandante en el sentido de que se debe tener en cuenta el conocimiento y la intención del programador del programa en cuestión cuando se escribió ese programa o la parte relevante del mismo.

En definitiva, el criterio aceptado por el tribunal fue remitirse al estado mental de la persona que programó el sistema automatizado; es decir, antes de que se formara el contrato. El criterio rechazado por el tribunal consistía en remitirse al estado mental que habría tenido la parte que operaba el sistema automatizado si hubiera conocido las circunstancias pertinentes que rodeaban la formación del contrato[26]. Estos criterios se pueden describir en los términos de que la ley puede exigir que el estado mental de una persona se determine subjetivamente, en función de lo que la persona sabe realmente o de su verdadera intención, u objetivamente, en función de lo que la persona parece saber o de su aparente intención[27].

Estos objetos o activos digitales no son cosas tangibles ni son fácilmente reclamables. Ahora bien, pueden representar, registrar o estar vinculados a otras cosas que son externas a ese token criptográfico y/o sistema de token

26. SENG, D., "Quoine Pte. v. B2C2 Ltd., recurso de apelación civil núm. 81 de 2019, sentencia de 24 de febrero de 2020", *Singapore Law Reports*, vol. 2020, núm. 2, págs. 44 a 69.

27. UNCITRAL, *Uso de la inteligencia artificial y la automatización en la contratación*, Nueva York, 4 a 8 de abril de 2022, pág. 2.

criptográfico en particular. Además, cualquier derecho de propiedad sobre ellas puede hacerse valer mediante el uso y disfrute de la cosa. Esta es una de las innovaciones fundamentales subyacentes de los criptotokens, porque todo se logra a través de *software*. En este contexto el Tribunal de Apelaciones de Inglaterra y Gales ha dicho que "un criptoactivo como bitcoin es una propiedad" según la legislación de Inglaterra y Gales[28].

Los tribunales de otras jurisdicciones han llegado a la misma (o similar) conclusión. Los tribunales de Australia, Canadá, Hong Kong, Nueva Zelanda, Singapur y Estados Unidos ahora proceden sistemáticamente sobre la base de que las criptomonedas pueden ser objeto de derechos de propiedad personal y, por lo tanto, son susceptibles de ser objeto de las diversas consecuencias que se derivan. Esto incluye el reconocimiento de que los criptotokens pueden estar sujetos a una orden judicial interlocutoria de propiedad, pueden mantenerse en fideicomiso y caen dentro de ciertas definiciones legales amplias de "propiedad".

En Hong Kong, en el caso Re Gatecoin Ltd (in liquidation) [2023] HKCFI 914[29] determino que las criptomonedas entran dentro de la definición de propiedad. En este sentido en Nueva Zelanda en el asunto Ruscoe v. Cryptopia Ltd [2020] NZHC[30] concluyó que las criptomonedas cumplían los cuatro criterios de "propiedad" establecidos en la decisión inglesa de National Provincial Bank v. Ainsworth [1965] AC 1775[31], sosteniendo que eran "definibles", ya que la clave pública asignada a una billetera de criptomonedas es fácilmente identificable, suficientemente distinta y capaz de ser asignada de manera única a los titulares de cuentas individuales; "identificables por terceros" ya que solo el titular de una clave privada puede acceder y transferir la criptomoneda de una billetera a otra; "capaz de ser asumidas por terceros" en el sentido de que puede ser y es objeto de mercados de comercio activos; y tiene "cierto grado de estabilidad" ya que toda la historia de vida de una criptomoneda está registrada en la blockchain. Por otro lado, el Tribunal de apelaciones de Singapur, en el asunto Quoine Pte. Ltd. V B2C2 Ltda. [2020] SGCA[32] dejó abierta la cuestión de cuál era

28. Tulip Trading contra Van Der Laan [2023] EWCA Civ 83, [2023] 4 WLR 16 en [24]-[25], por Birss LJ, quien también describió la cosa con la que se puede relacionar el derecho de propiedad. Tulip Trading contra Van Der Laan [2023] EWCA Civ 83, [2023] 4 WLR 16 en [24]-[25], por Birss LJ, quien también describió la cosa con la que se puede relacionar el derecho de propiedad.
29. Asunto [2023] HKCFI 914.
30. Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728; [2020] 2 NZLR 809 (8 April 2020)
31. National Provincial Bank v Ainsworth [1965] A.C. 1175.
32. COURT OF APPEAL of the republic of Singapore [2020] SGCA(I) 02

la naturaleza precisa del derecho de propiedad, ya que estaba convencido de que las criptomonedas podían tratarse como propiedad en un sentido genérico. De esta forma, afirma que puede decirse que las criptomonedas deberían poder subsumirse en los conceptos generales de los bienes, reconociendo al mismo tiempo que se plantean interrogantes complejos en cuanto al tipo de bien de que se trata.

En Copytrack Pte Ltd v Wall [2018] BCSC 1709[33], la Corte Suprema de Columbia Británica ordenó que se rastrearan ETH por valor de unos 400.000 dólares canadienses, lo que sugiere que ETH fue reconocido como una especie de propiedad susceptible de rastreo. La acción fue iniciada por Copytrack Pte Ltd ("Copytrack"), una empresa dedicada al negocio de gestión de contenido digital y aplicación automatizada de derechos de autor. Copytrack creó su propia criptomoneda, los tokens Copytrack, y transfirió por error una criptomoneda más valiosa, ETH, al inversor demandado en lugar de los tokens Copytrack. Luego, el demandado transfirió la ETH a terceros. Copytrack rastreó y recuperó el ETH. El tribunal caracterizó la cuestión conforme a un derecho de propiedad aplicado a las criptomonedas. En este sentido, el tribunal determina que, aunque no hay de acuerdo en cuanto a la naturaleza precisa de este derecho de propiedad sugiere (en el párrafo 182) que los titulares de tokens digitales como ETH deberían considerarse como propietarios, porque poseen un conjunto de derechos que incluyen el derecho a controlar el token. Este interés es identificable a través de entradas en la cadena de bloques, puede transferirse y tiene un alto grado de permanencia y estabilidad.

En Inglaterra, donde "la ley se ha mostrado renuente a tratar los datos en sí misma como un bien". En este sentido, el Tribunal de Apelación confirmó, recientemente, en el caso *Your Response Ltd. v. Datateam Business Media Ltd.*, que los datos almacenados en una base de datos electrónica no eran un bien corporal a los efectos del *common law* inglés y que, por lo tanto: a) los datos no podían ser objeto de un derecho de retención (es decir, el derecho del depositario a negarse a devolver el bien); y b) la retención de datos no podía ser objeto de una acción reivindicatoria (es decir, una demanda por actos indebidos de posesión o disposición de un bien ajeno). No obstante, el tribunal admitió que había argumentos sólidos a favor del reconocimiento de los objetos incorporales, por ejemplo, el material digitalizado, como una nueva categoría de bienes, aunque añadió que para introducir esa innovación jurídica sería necesario que interviniera el Parlamento.

33. Copytrack Pte Ltd. v. Wall 2018 BCSC 1709.

En algunos estados de EE. UU. se ha aceptado que la acción reivindicatoria se extienda a los objetos incorporales, por ejemplo, en el caso *Thyroff v. Nationwide Mutual Insurance Co.*, donde el Tribunal de Apelaciones del estado de Nueva York sostuvo que una acción reivindicatoria entablada al amparo de la legislación de dicho estado abarcaba los documentos electrónicos almacenados en una computadora, que no se distinguían de los documentos impresos, lo que en ese caso comprendía información de clientes e información personal almacenada en el sistema informático de un mandante al que un mandatario podía acceder a través de una computadora con licencia. No obstante, el tribunal advirtió que no había analizado si alguna de las otras, innumerables formas de información virtual debían ser protegidas por las normas de la responsabilidad civil extracontractual.

En la UE, parte de la doctrina jurídica ha entendido que el TJUE en su Sentencia de 3 de julio de 2012, en el asunto C-128/11, UsedSoft GmbH contra Oracle International Corp. abrió la puerta a un debate sobre la propiedad de los objetos incorporales. En ese asunto, el tribunal sostuvo que la distribución comercial de programas informáticos mediante descarga de Internet podía constituir una venta a los efectos de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador. Para llegar a esa conclusión, el tribunal consideró que, según una definición comúnmente aceptada, la "venta" era un contrato mediante el que "una persona transfiere a otra, a cambio del pago de un precio, los derechos de propiedad de un bien corporal o incorporal que le pertenece" y, por consiguiente, consideró que una "operación comercial que da lugar al agotamiento del derecho de distribución relativo a una copia de un programa de ordenador implica que se ha transferido el derecho de propiedad de esa copia" (apartados 44 y 45 de la Sentencia).

VI. AUTOMATIZACIÓN Y RESPONSABILIDAD: ATRIBUCIÓN DE ACTOS JURÍDICOS EN ENTORNOS ALGORÍTMICOS

En un contexto normal las partes redactaran el contrato *ex ante* para incluir todos los términos necesarios con respecto al cumplimiento, la formación, ejecución del contrato, la determinación del tribunal competente, la ley que se va a aplicar, etc. Ahora bien, en un entorno de contratación automatizada debemos hablar de un contexto de contratación en el que no existen lazos comerciales preexistentes, por lo que podemos decir que se basan en el anonimato de las partes. Ante esto, existe la necesidad de crear mecanismos que proporcionen garantías a la contratación que se va a realizar.

Dicho lo anterior, podemos observar varios problemas. El primero es el relativo al o a los lenguajes de programación procedimentales, que tendrá especificar cómo resolver un problema de manera clara y pertinente, determinado como se va a interpretar y ejecutar el contrato. Para ello se introducirán cláusulas y reglas establecidas en lenguaje informático a modo de código fuente y, por lo tanto, serán legalmente exigibles y podrían incluir cualquier cláusula, que las partes involucradas consideren necesaria.

En este sentido, pensemos que los errores de automatización, ya sean errores humanos (por ejemplo, en la programación del sistema) o errores que se producen en el procesamiento de datos (por ejemplo, el ingreso de datos erróneos de una fuente externa, los problemas de funcionamiento del sistema o la interferencia de terceros), que pueden llegar a exponer a las partes a cuantiosas pérdidas, lo cual, en el caso de las plataformas en línea, puede significar una pérdida del control de los activos digitales, una pérdida de ingresos o una pérdida de datos, lo que nos va a llevar claramente a supuestos de responsabilidad.

Los errores descritos pueden hacer incurrir en responsabilidad a las partes de contrato, al usuario final o a terceros proveedores de programas informáticos frente a la parte que utilizó el sistema para formar o ejecutar el contrato. La responsabilidad puede ser contractual (incumplimiento de las especificaciones de un contrato de suministro del programa informático) o extracontractual (incumplimiento culposo de la obligación de desarrollar el programa informático o responsabilidad por defectos del producto en el caso de los dispositivos "inteligentes")[34]. En este contexto, es donde nos centraremos a la hora de determinar la ley aplicable. En un contexto en el que los sistemas de Inteligencia Artificial (en adelante, IA) son sistemas deterministas[35] (es decir, los sistemas pueden automatizarse), donde será necesario evaluar el conocimiento en el momento de la programación y por referencia al programador. Esto puede ser problemático en los casos en que un programa relevante se ha hecho por otro programa[36].

Ahora bien, es importante señalar, aunque en este trabajo no se profundice, por lo que serán objeto de estudio en un futuro, que es posible que los

34. UNCITRAL, *Continuación de la labor relativa a la contratación automatizada*, Nueva York, 10 a 14 de abril de 2023.
35. ALPER, G., "Contract law revisited: Algorithmic pricing and the notion of contractual fairness", *Computer Law & Security Review*, Vol 47, Noviembre, 2022, págs. 21 a 67.
36. PENG, X., "A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends", *Computers and Electronics*, Vol. 208, Mayo, 2023, págs. 1 a 17.

principios del derecho vigentes no contemplen lo suficiente las cuestiones novedosas relacionadas con la imprevisibilidad de los sistemas automatizados que funcionan de manera no determinista, en el sentido de que no siempre generan el mismo producto con los mismos datos. Nos referimos a sistemas verdaderamente autónomos, que pueden dar lugar a investigaciones extremadamente complejas, y los sistemas de computación probabilística (es decir, la computación que se basa en una probabilidad de que algo sea la respuesta correcta, sin ser ni determinista ni autónomo), es decir, sistemas de computación cuántica[37].

En cualquier caso, adentrándonos en nuestro estudio, la naturaleza específica de los contratos automatizados no hay duda de que plantean cuestiones sobre ley aplicable en caso de responsabilidad contractual o extracontractual. Observemos que, en un contrato automatizado, con el uso de la IA, va a ser necesario observar los actores que participan o pueden verse afectados por el sistema, a los efectos del análisis jurídico[38]:

a) El desarrollador: persona responsable del diseño teórico de alto nivel del sistema de IA, así como de la programación, la capacitación y la verificación de dicho sistema.

b) El proveedor de datos: persona que proporciona datos al sistema (es decir, los datos necesarios para respaldar la capacitación, la implantación o el funcionamiento).

c) El implantador: persona que implanta el sistema integrándolo en sus operaciones (por ejemplo, en los bienes y servicios que suministra.

d) El operador: la persona que hace funcionar el sistema.

e) La persona afectada.

A los anteriores se le pueden sumar, en un sistema de registro distribuido los siguientes participantes[39]:

a) Un desarrollador: persona o grupo de personas que diseñan, desarrollan y mantienen el código informático con el que se hace funcionar el sistema.

---

37. ZIOUI, N., "Quantum computing based state domain equations and feedback control", *Results in Applied Mathematics*, Vol. 19, junio, 2023.
38. UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: la inteligencia artificial*, Nueva York, 6 a 17 de julio de 2020, pág. 5 y 6.
39. UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: continuación de la labor relativa a la contratación automatizada y progresos en otros aspectos*, Nueva York, 27 de junio a 15 de julio de 2022, pág. 2.

b) Un operador del nodo: persona que opera un nodo (es decir, una computadora que ejecuta el código informático).

c) Un administrador que controla: qué personas operan un nodo y qué operaciones realiza cada nodo.

La gama de actores descrita puede coincidir o no. En cualquier caso, pueden surgir relaciones contractuales entre la persona que implementa el sistema de IA y la persona que lo opera (por ejemplo, un contrato de suministro de bienes con IA integrada) o entre la persona que opera el sistema de IA y alguien afectado por él (por ejemplo, mediante un acuerdo de uso para la provisión de servicios con IA integrada). En ambos casos, el aprendizaje automático y los macrodatos pueden plantear desafíos para la aplicación de las normas contractuales existentes, especialmente en lo que respecta a determinar si ha ocurrido un incumplimiento del contrato y establecer el vínculo causal con el perjuicio ocasionado. Por ello, las partes involucradas en el contrato deben enfrentarse a la incertidumbre sobre un nivel de diligencia debida en la creación de algoritmos y la responsabilidad potencial por posibles fallos en el funcionamiento del sistema. Además, es posible que no puedan predecir los comportamientos del programa informático en un futuro ni ejercer control sobre la forma en que se utilizará el sistema de IA y cómo afectarán los datos nuevos que se ingresen en el programa en un determinado momento *a posteriori*[40].

Por ello, ante esto, la realización de los contratos automatizados plantea un riesgo importante, que consiste en ver cómo la responsabilidad se diluye respecto de las operaciones llevadas a cabo por las partes, si los criterios de aplicabilidad de la legislación no están lo suficientemente claros, motivo por el que pensamos en la necesidad de plantear posibles soluciones al problema de ley aplicable planteado.

VII. CONCLUSIONES

Conforme a lo anterior, debe profundizarse en el tráfico jurídico informático. Por ello, si partimos de la validez del Derecho preexistente y el principio de equivalencia funcional, no partimos de cero, ya que el derecho existente sirve para ser adaptado al derecho actual y que el mundo real sirve para adaptar al mundo virtual. Con ello, nos encontramos con que el derecho civil ofrece protección en caso de posesión o disposición indebida del bien corporal que contiene los bienes digitales; cuando la información registrada

40. UNCITRAL, *Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial: documento presentado por Chequia*, Nueva York, 25 de junio a 13 de julio de 2018, pág. 4.

en el bien digital se obtiene quebrantando el deber de confidencialidad o infringiendo las normas sobre privacidad; o cuando el bien digital está sujeto a un contrato, un derecho de autor o una patente.

Sin embargo, sería posible adquirir bienes digitales en circunstancias en que esa protección no fuese aplicable, como en el caso de que un hacker eliminara a distancia, de los servidores de una empresa, un programa informático no confidencial, pero valioso. Los bienes digitales pueden tener un inmenso valor comercial en el mundo moderno, lo que significa que existe una importante razón económica para garantizar que la ley proteja debidamente esos bienes.

BIBLIOGRAFÍA

ALPER, G., "Contract law revisited: Algorithmic pricing and the notion of contractual fairness", *Computer Law & Security Review*, Vol 47, noviembre, 2022, págs. 21 a 67.

AZIZ, A.; TELANG, R., "What Is a Digital Cookie Worth?", *SSRN*, marzo, 2016, págs. 3 a 37.

CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J., *Derecho Internacional Privado*, vol. II, 18.ª Ed., Comares, Granada, 2018, p. 1363.

CÁMARA LAPUENTE, S., *La sucesión mortis causa en el patrimonio digital: una aproximación*, conferencia dictada en el colegio notarial de Madrid, salón académico, el 24 de enero de 2019.

CUERVA DE CAÑAS, J. A., "La propiedad intelectual en el mundo digital", en *Sociedad Digital y Derecho* (Tomás de la Quadra-Salcedo y Fernández del Castillo (Dir.), José Luis Piñar Mañas (aut.), Ministerio de Industria, Comercio y Turismo, 2018, págs. 719 a 740.

DE MIGUEL ASENSIO, P. A., "Mercado único digital y propiedad intelectual: las Directivas 2019/789 y 2019/790", *La Ley Unión Europea*, número 71, 2019, pág. 21 a 56.

DIXIT, A., "Towards user-centered and legally relevant smart-contract development: A systematic literature review", *Journal of Industrial Information Integration*, Vol. 26, marzo, 2022, págs. 2 a 45.

FERRO, E., "Digital assets rights management through smart legal contracts and smart contracts", *Blockchain: Research and Applications*, junio, 2023, págs. 23 a 45.

FOSCH VILLARONGA, E.; KIESEBERG, P. ; LI, T., "Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten", *Computer Law & Security Review*, vol. 34, núm. 2, 2018, págs. 304 a 313.

GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la era de las big data y de la computación ubicua*, Dykinson, Madrid, 2016, p. 106.

JANEČEK, V., "Ownership of personal data in the Internet of Things", *Computer Law & Security Review*, núm. 34, 2018, pp. 1039-1052.

MADRID PARRA, A., "La identificación electrónica", *Revista de la Contratación Electrónica*, núm. 15, 2001, págs. 5 a 61.

MASON, S., *Electronic Evidence*, University of London Press, Londres, 2021.

MERCHAN MURILLO, A., "Sucesión digital internacional y el Reglamento sucesorio europeo 650/2012", *Anuario Español de Derecho Internacional Privado*, N.º 21, 2020, págs. 327-357.

PABÓN CADAVID, J., "Protección legal a los metadatos y la gestión digital de los derechos de autor", *Ius et Praxis*, Vol. 26, núm. 1, 2020, págs. 57 a 76.

PENG, X., "A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends", *Computers and Electronics*, Vol. 208, mayo, 2023, págs. 1 a 17.

PINHO, D., "What about the usability in low-code platforms? A systematic literature review", *Journal of Computer Languages*, Vol. 74, enero 2023, págs. 65 a 101.

PRINS, J.E.J., "The propertization of personal data and identities", *E.J.C.L.*, núm. 8, 2004, págs. 3 a 25.

SCHMIDT-KESSEN, M. J., "Machines that make and keep promises — Lessons for contract automation from algorithmic trading on financial markets", *Computer Law & Security Review*, Vol. 46, septiembre 2022, págs. 206 a 265.

SENG, D., "Quoine Pte. v. B2C2 Ltd., recurso de apelación civil núm. 81 de 2019, sentencia de 24 de febrero de 2020", *Singapore Law Reports*, vol. 2020, núm. 2, págs. 44 a 69.

UNCITRAL, Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial: documento presentado por Chequia, Nueva York, 25 de junio a 13 de julio de 2018.

UNCITRAL, Cuestiones jurídicas relacionadas con la economía digital: la inteligencia artificial, Nueva York, 6 a 17 de julio de 2020.

UNCITRAL, Cuestiones jurídicas relacionadas con la economía digital: continuación de la labor relativa a la contratación automatizada y progresos en otros aspectos, Nueva York, 27 de junio a 15 de julio de 2022.

UNCITRAL, Continuación de la labor relativa a la contratación automatizada, Nueva York, 10 a 14 de abril de 2023.

UNCTAD, *Informe sobre la Economía Digital 2019: Creación y captura de valor: repercusiones para los países en desarrollo*, Ginebra, 2019.

ZIOUI, N., "*Quantum* computing based state domain equations and feedback control", *Results in Applied Mathematics*, Vol. 19, junio, 2023.

Jurisprudencia

Seng, D., "*Quoine Pte. v. B2C2 Ltd.*", recurso de apelación civil n.º 81/2019, sentencia de 24 de febrero de 2020, *Singapore Law Reports*, vol. 2020, n.º 2, pp. 44-69.

UsedSoft GmbH vs. Oracle International Corp., Sentencia del TJUE de 3 de julio de 2012, asunto C-128/11.

Your Response Ltd. v. Datateam Business Media Ltd., Court of Appeal (England and Wales), 2014.

Thyroff v. Nationwide Mutual Insurance Co., New York Court of Appeals, 2007.

B2C2 Ltd. v. Quoine Pte Ltd., [2019] SGHC(I).

Ruscoe v. Cryptopia Ltd., [2020] NZHC.

Re Gatecoin Ltd (in liquidation), [2023] HKCFI 914.

Copytrack Pte Ltd v. Wall, [2018] BCSC 1709.

Capítulo 12

El refuerzo de la cooperación directa entre los Estados y los prestadores de servicios para la obtención de pruebas electrónicas en el Segundo Protocolo adicional al Convenio de Budapest*

Patricia Llopis Nadal
Prof.ª Permanente Laboral de Derecho Procesal
Universitat de València

SUMARIO: I. INTRODUCCIÓN. II. LA SOLICITUD DE DATOS DE SUS ABONADOS A LOS PROVEEDORES DE SERVICIOS: UNA MEDIDA DIRECTA DE ALCANCE NACIONAL PREVISTA EN EL ART. 18 DEL CONVENIO. III. LA COOPERACIÓN DIRECTA REFORZADA CON LOS PRESTADORES DE SERVICIOS EN EL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE BUDAPEST. 1. *Dos nuevos procedimientos para reforzar la cooperación directa con entidades y proveedores de servicios que se encuentran en el territorio de otros Estados parte*. 2. *La necesidad de respetar el principio de especialidad y el principio de proporcionalidad en los procedimientos de cooperación directa*. 3. *La autoridad competente para iniciar los procedimientos de cooperación directa: un concepto amplio que podría limitarse por los Estados parte*. 4. *El idioma de las solicitudes y de los requerimientos sujeto a lo que haya decidido la entidad o el proveedor de servicios requerido*. 5. *La necesaria protección de los derechos humanos, las libertades y los datos de carácter personal en la cooperación directa*. 5.1. La protección de los derechos humanos y de las libertades: la exigencia de respetar los

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro la autora.

niveles mínimos asumidos en virtud de tratados internacionales. 5.2. La protección de los datos de carácter personal: una exigencia regulada con detalle en el art. 14 del Segundo Protocolo en defecto de otro acuerdo aplicable. IV. LA POSIBILIDAD DE SOLICITAR INFORMACIÓN SOBRE LOS REGISTRANTES DE NOMBRES DE DOMINIO A LAS ENTIDADES UBICADAS EN EL TERRITORIO DE OTRO ESTADO PARTE. 1. *Facultar a sus autoridades y permitir a las entidades: la doble obligación asumida por los Estados parte en virtud del art. 6 del Segundo Protocolo*. 2. *Las entidades que prestan servicios de registro de nombres de dominio como receptoras de la solicitud y su condición de prestadores de servicios*. 3. *Los datos que pueden solicitarse a las entidades que prestan servicios de registro de nombres de dominio: relevancia y requisitos*. 4. *Los requisitos que ha de cumplir la solicitud y el necesario respeto de las garantías procesales en la entrega de la información*. V. LA POSIBILIDAD DE SOLICITAR INFORMACIÓN SOBRE LOS ABONADOS A LOS PROVEEDORES DE SERVICIOS QUE SE ENCUENTRAN EN EL TERRITORIO DE OTRO ESTADO PARTE. 1. *Las obligaciones asumidas en virtud del art. 7 del Segundo Protocolo y la posibilidad de reservarse el derecho a no aplicarlo de manera total o de manera parcial*. 1.1. La doble obligación que impone del art. 7 del Segundo Protocolo y la posibilidad de restringir las autoridades competentes de los otros Estados parte. 1.2. La posibilidad de realizar reservas de distinta extensión para la no aplicación del art. 7 por un Estado parte del Segundo Protocolo. 2. *Los proveedores de servicios definidos en el Convenio de Budapest como receptores del requerimiento*. 3. *La delimitación de los datos relativos a los abonados que pueden solicitarse a los proveedores de servicios*. 4. *El contenido mínimo del requerimiento y la posibilidad de acompañarlo de información complementaria*. 4.1. El contenido mínimo del requerimiento por el que se solicita a los proveedores de servicios información relativa a sus abonados. 4.2. La información complementaria al requerimiento y la necesidad de mayor claridad sobre cómo, quién, cuándo y qué habrá de aportarse. 5. *La posible intervención del Estado parte en cuyo territorio se encuentra el proveedor de servicios con carácter previo a facilitar la información*. 5.1. La posibilidad de que el Estado parte exija notificación simultánea del requerimiento con carácter general o en determinados supuestos. 5.2. La posibilidad de que el Estado parte exija la consulta previa del proveedor de servicios en determinados supuestos. 5.3. Las distintas actuaciones de la autoridad del Estado parte notificada simultáneamente o consultada por el proveedor de servicios. 6. *La negativa o inactividad del proveedor de servicios y el recurso a la cooperación internacional o a la asistencia mutua como alternativa*. 6.1. Las posibles conductas del proveedor de servicios requerido y la posibilidad de exigir que motive toda negativa e

inactividad. 6.2. Las alternativas de la autoridad competente para obtener la información ante la negativa o inactividad del proveedor de servicios. VI. CONCLUSIÓN. BIBLIOGRAFÍA Y OTRAS FUENTES CONSULTADAS. 1. *Bibliografía*. 2. *Otras fuentes consultadas*.

I. INTRODUCCIÓN

El Convenio sobre la Ciberdelincuencia[1] (en adelante, el Convenio) fue adoptado en el seno del Consejo de Europa en el año 2001 —siendo el primer tratado internacional sobre la materia y el que mayor éxito ha tenido[2]—. Conocido también como el Convenio de Budapest, su objetivo es proteger a la sociedad frente a los delitos cometidos en el entorno digital y, para ello, se centra en tres aspectos esenciales: establecer una regulación común de derecho penal sustantivo en materia de ciberdelitos, armonizar el derecho procesal respecto de la obtención de pruebas electrónicas y la jurisdicción competente y fijar normas de cooperación internacional en la lucha contra la ciberdelincuencia que respondan a la rapidez y eficacia que exige este ámbito[3].

Pese a que el texto fue redactado en una organización de ámbito regional, como afirma GASCÓN MARCÉN "tiene una auténtica vocación universal más allá del entorno europeo"[4]. En este sentido destaca, en especial, el elevado número de Estados que lo han ratificado —un total de setenta y ocho[5]—, entre los que se incluyen, junto a los Estados del Consejo de

1. Convenio sobre la Ciberdelincuencia, Serie de Tratados del Consejo de Europa, n.º 185, de 23 de noviembre de 2001.
2. GASCÓN MARCÉN, A., "The Budapest Convention and the UN Cybercrime Convention negotiations", en SEGURA SERRANO, A., *Global cybersecurity and International Law,* Routledge, 2024, p. 175.
3. ASENCIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", en FERNÁNDEZ LÓPEZ, M. y ASENCIO MELLADO, J. M, *Justicia penal y nuevas formas de delincuencia,* Tirant lo Blanch, 2017, pp. 46 y ss.; BUJOSA VADELL, L., "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", en FONTESTAD PORTALÉS, L. y JIMÉNEZ LÓPEZ, M. N., *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Thomson Reuters-Aranzadi, 2022, pp. 74 a 77.
4. Añade la autora que esta vocación universal tiene sentido "puesto que la ciberdelincuencia es por su propia naturaleza en la mayoría de los casos transnacional" [GASCÓN MARCÉN, A., "La mejora de la obtención de pruebas electrónicas: avance necesario para la seguridad europea", en *La Unión Europea y la seguridad: defensa de los espacios e intereses comunes,* ICEI Ocassional Papers, 2018, p. 19].
5. Según la página web del Consejo de Europa, en el momento en que se redactaron estas líneas el total de Estados parte del Convenio era de setenta y ocho (disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, última consulta, 23 de abril de 2025).

Europa —con la excepción de Irlanda—, otros tan diversos como Australia, Brasil, Costa Rica, Estados Unidos, Ghana, Japón o Sierra Leona[6] —siendo particularmente significativo el hecho de que formen parte del Convenio Estados muy desarrollados tecnológicamente[7]—.

Como apunta VELASCO NÚÑEZ, entre los aspectos positivos del Convenio debe mencionarse que, aunque afecta a una materia muy cambiante, no se ha visto superada por esta gracias a que "acepta el sistema de *actualizaciones* a través de sus Protocolos adicionales"[8]. Así, a inicios del año 2003 —apenas transcurrido un año desde que se acordará el Convenio— tuvo lugar su primera actualización mediante el Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos[9]. Por su parte, la segunda y más reciente actualización se produjo dos décadas después de la adopción del Convenio mediante el Segundo Protocolo adicional relativo a la cooperación reforzada y la revelación de pruebas electrónicas[10] (en adelante, el Segundo Protocolo)[11];

6. "Este tratado está abierto a la adhesión por cualquier Estado. El hecho de que el Convenio de Budapest fuera negociado no solo por los Estados miembros del Consejo de Europa, sino también por Estados Observadores, fue clave para su éxito. Esto se debe a que permitió que el Convenio se adaptara a las necesidades de un mundo globalizado, donde los ciberdelitos no conocen fronteras" [JARIEGO RUIZ, M.ª "Ciberdelincuencia: amenaza en la red y la oportunidad del Convenio de Budapest", *Diario La Ley*, núm. 10358 (2023), p. 7].
7. VELASCO NÚÑEZ, E., "El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", *Diario La Ley*, núm. 62 (2022), p. 2.
8. *Ibidem*, p. 1.
9. Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, Serie de Tratados del Consejo de Europa, n.º 189, de 28 de enero de 2003. Según la página web del Consejo de Europa, en el momento en que se redactaron estas líneas el total de Estados que habían ratificado el Protocolo adicional era de treinta y siete (disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189, última consulta, 24 de abril de 2025).
10. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la revelación de pruebas electrónicas, Serie de Tratados del Consejo de Europa, n.º 224, de 12 de mayo de 2022. Según la página web del Consejo de Europa, en el momento en que se redactaron estas líneas el total de Estados que habían firmado el Segundo Protocolo adicional era de cuarenta y siente, siendo dos —Serbia y Japón— quienes lo habían ratificado (disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, última consulta, 24 de abril de 2025). Desde el 12 de mayo de 2022, España se incluye entre los países que han firmado el Segundo Protocolo.
11. Sobre el camino seguido hasta la adopción del Segundo Protocolo, *vid*., BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest: Nuevos medios para la cooperación penal y la obtención de prueba electrónica", *La Ley Penal*,

para cumplir con su objetivo este Protocolo se centra en cuatro procedimientos distintos: (1) la cooperación directa con los proveedores de servicios ubicados en el territorio de otro Estado —arts. 6 y 7— (2) la cooperación internacional entre autoridades para la entrega de datos —arts. 8 y 9— (3) la asistencia mutua en situaciones de emergencia —art. 10— y (4) la cooperación internacional en materia de videoconferencias y equipos conjuntos de investigación cuando no haya un tratado internacional aplicable —arts. 11 y 12—, todo esto, con la garantía de respetar los derechos humanos y las libertades y de proteger los datos de carácter personal —arts. 13 y 14—[12].

El presente trabajo se centra en el estudio de las novedades introducidas por el Segundo Protocolo en materia de *cooperación directa* entre las autoridades competentes y los proveedores de servicios que poseen la información[13]. En otras palabras, el objeto de esta investigación son los procedimientos introducidos por los arts. 6 y 7 del Segundo Protocolo, los cuales permiten a la autoridad de un Estado que requiere determinada prueba electrónica a efectos de una causa penal solicitar tal información a prestadores de servicios ubicados fuera de su jurisdicción —una solicitud transfronteriza dirigida a un ente de naturaleza privada que se articula sin que intervenga autoridad alguna del Estado en cuyo territorio se encuentra el prestador de servicios—[14]. Este análisis se realiza teniendo en cuenta que son los propios

---

núm. 157 (2022), pp. 2 y 3; GASCÓN MARCÉN, A., "Improving access to electronic evidence: the European normative struggle", en *Cybercrime: new threats, new responses: Actas del XV.º Congreso Internacional Internet, Derecho y Política,* Universitat Oberta de Catalunya, 2020, pp. 148-150.

12. DELGADO MARTÍN, J., "Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", *Diario La Ley*, núm. 10358 (2023), pp. 5 a 7.

13. Nota de la autora: si bien las versiones en español del Convenio y del Segundo Protocolo —publicadas, respectivamente, en el BOE y en el DOUE—, utilizan el término *proveedor de servicios*, en este trabajo también se utiliza la expresión *prestador de servicios* —más acorde con la terminología utilizada en las recientes normas de Derecho de la Unión Europea, *vid*., entre otros, Reglamento (UE) 2022/2065, de 19 de octubre de 2022 o Reglamento (UE) 2023/1543, de 12 de julio de 2023—. Asimismo, se ha optado por el uso de la expresión *prestadores de servicios* en el título del trabajo, por considerar que en la misma cabe incluir tanto a las entidades a las que se refiere el art. 6 del Segundo Protocolo, como a los proveedores a los que se refiere el art. 7.

14. SIGNORATO, S., "Cross-border gathering of e-evidence: different legal frameworks in European Union and Council of Europe", *Journal of Eastern European Criminal Law*, núm. 1 (2023), pp. 15 y 16, sintetiza de manera clara las tres ideas esenciales sobre los proveedores de servicios como sujetos imprescindibles en esta cooperación directa introducida por el Segundo Protocolo: "juegan un papel fundamental también en el plano jurídico […] procesan información que podría convertirse en prueba en un proceso penal", "su colaboración se requiere en las investigaciones […] siendo impor-

Estados parte quienes, en cumplimiento de las obligaciones asumidas en virtud de este tratado internacional, deberán introducir medidas de carácter procesal en sus ordenamientos jurídicos internos —como ya hicieron a partir del Convenio de 2001— para garantizar que puede articularse la cooperación directa en una doble dirección: de sus autoridades con los prestadores de otro Estado y de los prestadores que se encuentran en su territorio con las autoridades de otro Estado.

II. LA SOLICITUD DE DATOS DE SUS ABONADOS A LOS PROVEEDORES DE SERVICIOS: UNA MEDIDA DIRECTA DE ALCANCE NACIONAL PREVISTA EN EL ART. 18 DEL CONVENIO

Como parte de la sección destinada a las cuestiones de derecho procesal, el Convenio introdujo en su art. 18 la denominada "orden de presentación"; en virtud de esta disposición, los Estados parte asumieron la obligación de adoptar medidas legislativas para facultar a sus autoridades a ordenar la entrega de determinados datos a dos tipos de sujetos. De un lado, a las personas que se encuentran en su territorio, para que entreguen datos informáticos que posean o que estén bajo su control. De otro lado, a los proveedores de servicios que ofrecen prestaciones en su territorio, para que comuniquen los datos —informáticos o analógicos—, relativos a sus abonados en relación con el servicio que les prestan. Asimismo, la disposición es categórica al determinar los datos que pueden solicitarse a estos sujetos, excluyendo de un modo expreso tanto los datos de tráfico[15] como los datos de contenido[16].

Como se ha anticipado, la segunda previsión —regulada en el art. 18.1.b)— permite la solicitud de datos de sus abonados a los proveedores de servicios[17], sin embargo, aunque la relación entre la autoridad y el prestador

---

tante la cooperación entre los Estados y el sector privado […] el cual, con frecuencia, se convierte en esencial", "esta cooperación también se caracteriza por aspectos problemáticos […] los prestadores operan conforme a la lógica de los negocios, concediendo a la justicia una importancia secundaria […] surgen nuevos retos pues siempre es necesario verificar la compatibilidad de la recogida de pruebas con las garantías procesales" (traducción libre de la autora).

15. Conforme a la definición que realiza el art. 1.d) del Convenio, se trata de datos informáticos relativos a una comunicación que proporcionan información sobre el origen, destino, fecha, duración… de esta.
16. No se definen en el Convenio, pero se trata de los textos, vídeos, imágenes, sonidos, voz… que integran la comunicación transmitida mediante un sistema informático.
17. Apunta DE HOYOS SANCHO "La posibilidad de obtener directamente de los proveedores de servicios información sobre los datos de abonados ya se encontraba en

es directa, se trata de una medida exclusivamente nacional, que no habilita para llevar a cabo una *cooperación directa* —entendida como las solicitudes de entrega de datos de carácter transfronterizo—[18], aunque tampoco la impide si el proveedor de servicios requerido carece de obstáculos legales y lo considera oportuno[19]. En consecuencia, cuando era necesario obtener datos en poder de proveedores de servicios ubicados en otra jurisdicción, estos solo podían solicitarse mediante el recurso a los instrumentos tradicionales de cooperación internacional[20] —ahora bien, como exponemos *infra* los términos utilizados en este artículo podrían dar lugar a pensar en un ámbito de aplicación más extenso que el meramente interno—[21].

A pesar de que todavía no era posible hablar de una cooperación directa, no podemos negar la relevancia del art. 18 para el objeto de este trabajo, pues su apartado tercero, donde se define el concepto "datos relativos a los abonados", ha sido utilizado dos décadas después a efectos de delimitar el ámbito de aplicación del art. 7 del Segundo Protocolo. Además, la expresión "obren en su poder o estén bajo su control", utilizada en el art. 18 —y explicada en

---

el art. 18 del propio Convenio de Budapest de 2001, pero se excluía expresamente la posibilidad de que estos proveedores ofrecieran datos sobre el tráfico" [DE HOYOS SANCHO, M., "Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo", *Revista de Estudios Europeos*, núm. extraordinario monográfico (2023), p. 119].

18. "Los supuestos que están amparados por el Convenio de Budapest tienen un ámbito doméstico. Mediante el recurso al artículo 18 del Convenio […] Fuera de estos supuestos, la cooperación directa con proveedores radicados en países distintos de aquel que necesitara la información almacenada venía siendo voluntaria para el proveedor" [BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 5].
19. "La posibilidad de obtener directamente información sobre los datos de abonado ya estaba prevista en el artículo 18 de la Convención, pero con carácter voluntario para el proveedor, que podía facilitar o no esa información, sin que el Estado en el que el proveedor se encontraba ubicado tuviera intervención alguna al respecto" [TEJADA DE LA FUENTE, E., Entrevista — Ciberderecho, *Diario La Ley*, 24 de mayo de 2022, p. 4].
20. En este sentido, GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., "El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad", *Revista General de Derecho Procesal*, núm. 58 (2022), p. 11. Mantiene el autor a propósito de la orden de presentación del art. 18 "La medida se queda en el orden interno, pero puede trascender al ámbito de cooperación internacional cuando estos datos sean solicitados por los medios tradicionales de cooperación".
21. Hacemos uso de verbos en pasado para referirnos al Convenio, en contraposición con las referencias al Segundo Protocolo que se realizan en presente, si bien en el momento en que se redactan estas líneas el art. 18 del Convenio sigue siendo la única disposición en vigor en materia de cooperación directa, pues para que se produzca la entrada en vigor Segundo Protocolo se requiere su ratificación por, al menos, cinco Estados parte —siendo dos, como se ha apuntado, los únicos que hasta la fecha lo han ratificado—.

el Informe que acompaña al Convenio[22]—, rige igualmente para el art. 6 y el art. 7 del Segundo Protocolo. Por último, respecto de esta orden introducida por el Convenio también se prevén cuestiones como su presentación por autoridades judiciales a efectos de garantizar los derechos humanos, la exclusión de los delitos menos graves por el principio de proporcionalidad o la posibilidad de exigir el respeto de su carácter confidencial[23].

Si bien ya hemos indicado que el art. 18 del Convenio se limita a supuestos estrictamente internos, debemos detenernos en la redacción de su apartado primero, letra b), donde permite exigir la entrega de los datos "a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte"[24]. Así, parece que pretende establecer una distinción entre *ofrecer servicios en el territorio del Estado* que le puede solicitar la entrega de los datos y *encontrarse en el territorio de ese Estado* —términos que sí utiliza la letra a), que se refiere a "persona que se encuentre en su territorio" —[25]; por lo que sería irrelevante en qué territorio se encuentra establecido el proveedor de servicios para que la autoridad del Estado parte pudiera pedirle la entrega de los datos si está, de algún modo, ofreciendo sus servicios en su territorio[26] —el alcance de la expresión "que ofrezca prestaciones en el territorio de esa Parte" fue objeto de aclaraciones por el Comité del Convenio sobre la Ciberdelincuencia transcurrida más de una década desde su adopción[27]—.

22. Informe explicativo al Convenio sobre la Ciberdelincuencia, apartado 173 (disponible en: https://rm.coe.int/16802fa403, última consulta, 20 de abril de 2025).
23. Informe explicativo al Convenio sobre la Ciberdelincuencia, apartados 174 y 175.
24. El Informe explicativo intenta acotar la extensión de la idea *ofrecer servicios* al concretar que se trata de "obtener información acerca de los abonados en relación con servicios ofrecidos en el territorio de la Parte que ordena la presentación de los datos" (Informe explicativo al Convenio sobre la Ciberdelincuencia, apartado 173 *in fine*).
25. Así, mientras que *encontrarse* es sinónimo de estar ubicado —de tener un establecimiento—, *ofrecer servicios* es algo que puede realizarse aunque el proveedor de servicios se encuentre —esté establecido— en otro Estado —y más en un ámbito de peculiares características como es el entorno digital—.
26. Estos términos fueron aclarados por la Nota orientativa n.º 10 del Comité del Convenio sobre la Ciberdelincuencia (T-CY) "el art. 18.1.b) no se pronuncia sobre la cuestión de la ubicación del proveedor de servicios. Las Partes podrían aplicar la disposición en circunstancias en las que el proveedor que ofrezca sus servicios en el territorio de la Parte no esté presente en su territorio ni jurídica ni físicamente" [T-CY (Cybercrime Convention Committee), Guidance note #10 Production orders for subscriber information (Article 18 Budapest Convention), T-CY(2015)16, 28 February 2017, p. 6 (disponible en: https://rm.coe.int/16806f943e, última consulta: 25 de abril de 2025)]. Sobre el art. 18.1.b) y el acceso a los datos que se encuentran físicamente en otra jurisdicción, *vid*., GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., "El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad", *op. cit.*, pp. 15 y 16.
27. T-CY (Cybercrime Convention Committee), Guidance note #10, p. 8.

A pesar de estos matices, el Convenio se adoptó en un momento muy temprano para pensar en una cooperación directa con entes de naturaleza privada ubicados fuera de la jurisdicción del Estado parte que solicita la entrega de los datos. Asimismo, no contiene la doble obligación que sí imponen los arts. 6 y 7 del Segundo Protocolo, consistente no solo en facultar a sus autoridades para la emisión de órdenes dirigidas a los proveedores de servicios ubicados en el territorio de otro Estado parte, sino, también, en adoptar las medidas legislativas necesarias a nivel nacional para permitir a los proveedores de servicios que se encuentran en su territorio revelar la información relativa a sus abonados a las autoridades de otro Estado parte —esta obligación es objeto de desarrollo *infra*—[28].

III. LA COOPERACIÓN DIRECTA REFORZADA CON LOS PRESTADORES DE SERVICIOS EN EL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE BUDAPEST

1. DOS NUEVOS PROCEDIMIENTOS PARA REFORZAR LA COOPERACIÓN DIRECTA CON ENTIDADES Y PROVEEDORES DE SERVICIOS QUE SE ENCUENTRAN EN EL TERRITORIO DE OTROS ESTADOS PARTE

El Preámbulo del Segundo Protocolo introduce con claridad tanto la situación existente como su propósito; así, con tres ideas sintetiza la necesidad y la importancia de esta nueva regulación. En primer lugar, no solo nos recuerda que cada vez es más frecuente que las pruebas de los delitos se almacenen en formato electrónico, sino que, además, apunta el problema de que estas se encuentren "en sistemas informáticos ubicados en países extranjeros, múltiples o desconocidos". En segundo lugar, asume que en este contexto es necesario establecer una "cooperación mayor y más eficiente entre los Estados y el sector privado", y no se olvida de que las entidades

28. A propósito de las diferencias del nuevo art. 7 del Segundo Protocolo con el art. 18 del Convenio, SIRIUS Project destaca el hecho de que el art. 7 ya no exija un vínculo territorial con el Estado parte que requiere los datos, por lo que va más allá del ámbito de aplicación del art. 18 del Convenio, el cual se limitaba a la posibilidad de que las autoridades competentes de un Estado parte ordenaran la entrega de datos a los proveedores que ofrecían sus servicios en el territorio de ese Estado parte [SIRIUS Project, Cross-border Access to electronic Evidence, "Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscribers information", last update: 23/01/2024, Eurojust — Europol, pág. 2 (disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/production-orders-for-the-disclosure-of-subscriber-information-under-article-7-of-the-second-additional-protocol-to-the-convention-on-cybercrime-23-01-2024.pdf, última consulta: 18 de abril de 2025)].

privadas que pueden proporcionar tales pruebas, en la medida en que van a recibir peticiones de datos de manera directa de autoridades de otro Estado, precisan de seguridad jurídica para saber cómo actuar. Y, en tercer lugar, se marca "el objetivo de seguir reforzando la cooperación" en materia de obtención de pruebas en formato electrónico, tanto la cooperación que se establece entre las autoridades de los Estados, como "la cooperación directa entre las autoridades competentes y los proveedores de servicios y otras entidades" que dispongan de la información requerida[29].

A efectos de lograr el propósito indicado en su preámbulo, el Capítulo II del Segundo Protocolo incorpora una Sección 2 titulada "Procedimientos que refuerzan la cooperación directa con proveedores y entidades en el territorio de otras Partes" e integrada por los arts. 6 y 7 donde se regulan sendas medidas de cooperación directa. Como primera medida, el art. 6 prevé que la autoridad de un Estado parte del Segundo Protocolo pueda solicitar a quien presta servicios de nombres de dominio en el territorio de otro Estado parte información que le permita identificar a la persona que ha registrado un dominio o ponerse en contacto con ella. El art. 7, a su vez, incorpora una segunda medida por la que la autoridad de un Estado parte puede requerir a los prestadores de servicios que se encuentren en el territorio de otro Estado parte información sobre sus abonados[30].

No hay duda del notable avance que suponen estos procedimientos de cooperación directa para la obtención de pruebas electrónicas —incluso cuando en la práctica esto se venía realizando de manera voluntaria[31]—, un progreso más que significativo, tanto por el relevante papel de estos entes de naturaleza privada cuando se trata de obtener la identidad de quien actúa

29. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, Preámbulo, párrafos 9.º a 11.º

30. Si existían dudas sobre la relación de los proveedores de servicios con la autoridad que puede solicitarles la entrega de la información —entre otras, las expuestas *supra* a propósito del art. 18 del Convenio—, estas han sido definitivamente clarificadas mediante el Segundo Protocolo [GASCÓN MARCÉN, A., "The push for the international regulation of cross-border Access to electronic evidence and human rights", *Cuadernos de Derecho Transnacional*, vol. 15, núm. 1 (2023), p. 399].

31. DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica en procesos penales: Análisis y valoración del "e-evidence package"*, Aranzadi-La Ley, Madrid, 2024, p. 134. Destaca la autora que con el Segundo Protocolo "se recogen en un instrumento normativo internacional, dotado de más garantías, algunas prácticas de cooperación transfronteriza en materia penal que ya se estaban llevando a cabo […] como las colaboraciones directas y voluntarias prestadas por algunos proveedores de servicios radicados fuera del territorio del Estado reclamante en relación con peticiones de datos de abonados o incluso de tráfico".

tras el anonimato que brinda internet —o para ponerse en contacto con esta persona—[32], como por la celeridad que se consigue al no tener que pasar por autoridades del Estado parte requerido que actúen como intermediarias. Por ello, como apunta BAHAMONDE BLANCO, estas medidas —las de los arts. 6 y 7, junto a la prevista en el art. 8—, constituyen "el mayor éxito del Protocolo"; además, justifica la relevancia de estos nuevos procedimientos con los siguientes términos: "sobre todo si nos centramos en el aspecto cuantitativo, esto es, el elevadísimo número de solicitudes de datos almacenados (esencialmente de abonado) que las autoridades encargadas de una investigación penal necesitan, frecuentemente incluso para poder iniciar una investigación"[33].

2. LA NECESIDAD DE RESPETAR EL PRINCIPIO DE ESPECIALIDAD Y EL PRINCIPIO DE PROPORCIONALIDAD EN LOS PROCEDIMIENTOS DE COOPERACIÓN DIRECTA

Antes de analizar detalladamente ambas medidas, es oportuno destacar los aspectos que tienen en común. Así, por exigencia del principio de especialidad, estos procedimientos de cooperación directa solo pueden solicitarse en el marco de un proceso penal para la investigación de un delito específico, requiriéndose en todo momento que la información se precise "para investigaciones o procesos penales específicos". En línea con el ámbito de aplicación del Segundo Protocolo —tal y como prevé su art. 2—, la solicitud de pruebas electrónicas puede realizarse en casos de ciberdelincuencia, así como, cuando sean relevantes, para todo tipo de delitos cometidos en el plano analógico.

El art. 2, en su apartado 1.a), establece que las medidas introducidas por el Segundo Protocolo "se aplicarán (…) a delitos relacionados con datos y sistemas informáticos, y a la obtención de pruebas electrónicas de cualquier delito", por ello, es oportuno consultar las aclaraciones del Informe explicativo al Segundo Protocolo, donde se concreta que la expresión "delitos relacionados con datos y sistemas informáticos" se refiere a los delitos contemplados en el art. 14.2.a) y b) del Convenio, esto es, respectivamente, todos los delitos previstos en los arts. 2 a 11 del Convenio y otros delitos

32. Sobre el carácter esencial de la colaboración de los prestadores de servicios para identificar a los autores del delito en el entorno digital, *vid*., GARCÍA SÁNCHEZ, M. D., *Medidas cautelares cibernéticas: una nueva oportunidad en la lucha contra la ciberdelincuencia*, Atelier, Barcelona, 2024, pp. 90 y 91.

33. BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 5.

cometidos por medio de un sistema informático —los denominados casos de ciberdelincuencia—[34]. Añade el art. 2.1.b) del Segundo Protocolo la posibilidad de que estas pruebas electrónicas se soliciten en procesos penales relativos a delitos tipificados en el Primer Protocolo (actos de índole racista y xenófoba cometidos mediante sistemas informáticos) y entre Estados que sean parte de ambos Protocolos.

Ahora bien, lo indicado en los párrafos precedentes está condicionado al respeto de la proporcionalidad, de modo que, en cuanto la obtención de tales pruebas supone una injerencia en los derechos fundamentales, solo podrán solicitarse cuando la naturaleza y las circunstancias del delito tengan entidad suficiente para justificar tal afectación —es decir, no podrá hacerse uso de estos procedimientos cuando se trate de delitos leves—. Asimismo, la necesidad de la información y su pertinencia para la causa penal, conforme a lo que establezca la legislación interna de cada Estado, también habrán de concurrir cuando se pidan estas pruebas electrónicas, no siendo posible en ningún caso reclamar la entrega generalizada e indiscriminada de datos[35].

3. LA AUTORIDAD COMPETENTE PARA INICIAR LOS PROCEDIMIENTOS DE COOPERACIÓN DIRECTA: UN CONCEPTO AMPLIO QUE PODRÍA LIMITARSE POR LOS ESTADOS PARTE

El Convenio definió algunos de los conceptos fundamentales en materia de cooperación y prueba electrónica —entre otros, el concepto de *proveedor de servicios* o el de *datos de los abonados*—, por este motivo, el art. 3.1 del Segundo Protocolo se remite expresamente a los arts. 1 y 18 del texto adoptado en 2001. Sin embargo, en este tratado internacional no encontramos una definición del término *autoridad competente*, siendo el Segundo Protocolo, en su art. 3.2.b), quien lo define por vez primera. Así, se entiende como tal toda autoridad judicial, administrativa o policial —encargada de hacer cumplir la ley—, a condición de que conforme a su derecho interno esté facultada para ordenar las medidas de cooperación que regula el Segundo Protocolo, para

34. Informe explicativo al Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas, Serie de Tratados del Consejo de Europa, n.º 224, de 12 de mayo de 2022, apartado 33 (disponible en: https://rm.coe.int/1680a83723, última consulta, 17 de abril de 2025).

35. Esto se matiza en el Informe explicativo al Segundo Protocolo, diferenciando entre los Estados parte del Convenio Europeo de Derechos Humanos y el resto de los Estados que no son parte de este tratado internacional, pero sí han ratificado el Segundo Protocolo (*vid*., Informe explicativo al Segundo Protocolo adicional, apartados 84 y 97).

autorizar tales medidas o para llevarlas a cabo y siempre que esa facultad la tenga atribuida a efectos de la obtención de pruebas en el marco de una investigación o de un proceso penal específico.

Se trata, por tanto, de un concepto amplio, que pretende atender a las distintas particularidades de los Estados que, previsiblemente, serán parte del Segundo Protocolo —incluyendo, con esta previsión, a jueces, fiscales, autoridades administrativas, cuerpos y fuerzas de seguridad u otros funcionarios públicos—. No obstante, se permite a los Estados formular una declaración por la que limiten este concepto de autoridad competente, como veremos, ello se prevé solo respecto de la medida de cooperación directa regulada en el art. 7 —solicitud de datos de los abonados— y para aquellos Estados parte en cuyo territorio se encuentre el prestador de servicios receptor de la solicitud —es decir, cuando sea el requerido—.

4. EL IDIOMA DE LAS SOLICITUDES Y DE LOS REQUERIMIENTOS SUJETO A LO QUE HAYA DECIDIDO LA ENTIDAD O EL PROVEEDOR DE SERVICIOS REQUERIDO

Las dos medidas de cooperación directa introducidas por el Segundo Protocolo se caracterizan por tener como receptores a entes de naturaleza privada. Son estos particulares, las entidades que prestan servicios de nombres de dominio y los proveedores de servicios, quienes deciden el idioma —o los idiomas— en que se deberá presentar la solicitud o el requerimiento dirigido a ellos.

Así, si la entidad o el proveedor no ha dispuesto otra cosa, la petición se presentará en el idioma del Estado parte en cuyo territorio se encuentre, que habrá de ser, además, el idioma utilizado en procedimientos internos comparables —esto es, cuando la autoridad de su propio Estado le pide información a efectos de una causa penal—. En el caso de que en el Estado parte haya más de una lengua oficial, se presentará en el idioma que la entidad o el proveedor acepte en los procedimientos nacionales comparables —entendiendo que puede ser uno o varios idiomas, según lo que el particular requerido suela aceptar—[36].

También es posible que la entidad o el proveedor de servicios acepte que las peticiones se presenten en otro idioma —normalmente, se tratará de una lengua franca, como el inglés, habitual en quienes desarrollan su negocio en el entorno digital[37]—. En tal caso, el idioma en que se presenta la solicitud o

36. Sobre esto, *vid.*, Informe explicativo al Segundo Protocolo adicional, apartado 58.
37. Informe explicativo al Segundo Protocolo adicional, apartado 50.

el requerimiento queda a elección de la autoridad competente que lo emite —pudiendo optar entre la primera o la segunda opción—.

Finalmente, nada impide que se presente en cualquier otro idioma, a condición de que se acompañe de una traducción al idioma utilizado en los procesos nacionales o, en su caso, al idioma aceptado por el propio particular requerido. Si bien esto se prevé como una alternativa más en el art. 4.2 del Segundo Protocolo —pudiendo elegir entre las dos que han sido expuestas en los párrafos anteriores o esta opción—, podría ser particularmente útil acompañar, en todo caso, el texto en el idioma de la autoridad que pide la información —sobre todo cuando la presentación en alguno de los idiomas que acepte la entidad o el proveedor se realice a partir de una traducción de los datos esenciales en el idioma oficial de la autoridad emisora—, esto permitiría resolver con mayor rapidez dudas sobre la interpretación de algunos extremos del requerimiento o solicitud.

Es de destacar, por tanto, que no se haya exigido el uso del inglés —u otro idioma— como lengua franca al establecer las comunicaciones con las entidades que prestan servicios de nombres de dominio y con los proveedores de servicios. De este modo, se da mayor libertad —y flexibilidad[38]— a los implicados en la cooperación directa —que podrían pertenecer a Estados parte con idiomas más similares entre sí que al inglés u a otra lengua franca preestablecida e, incluso, Estados que compartan el mismo idioma—, permitiendo que esto quede a elección de los particulares y que, en caso de ser distintos idiomas, la autoridad que emite la solicitud o el requerimiento decida cuál utilizar.

5. LA NECESARIA PROTECCIÓN DE LOS DERECHOS HUMANOS, LAS LIBERTADES Y LOS DATOS DE CARÁCTER PERSONAL EN LA COOPERACIÓN DIRECTA

5.1. La protección de los derechos humanos y de las libertades: la exigencia de respetar los niveles mínimos asumidos en virtud de tratados internacionales

El respeto de una serie de condiciones y salvaguardias es fundamental al establecer y ejecutar estas medidas de naturaleza procesal, por ello, el Segundo Protocolo destina el tercer capítulo, en su integridad, a regularlas en torno a dos cuestiones: la protección de los derechos humanos y las

38. BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 4.

libertades y la protección de los datos de carácter personal. En cuanto a los primeros, el art. 13 del Segundo Protocolo nos remite al art. 15 del Convenio, donde se prevé en qué deben consistir estas garantías; para los segundos, el art. 14 detalla en la disposición más extensa del Segundo Protocolo todos los extremos que afectan a esta necesaria protección.

Así, conforme al art. 15 del Convenio, también es obligación de los Estados parte del Segundo Protocolo asegurar que toda actividad relacionada con los procedimientos de cooperación directa se lleve a cabo sujeta a las garantías y salvaguardias de su ordenamiento jurídico, las cuales, necesariamente, habrán de proteger de un modo adecuado los derechos humanos y las libertades. En concreto, a pesar de las diferencias que puedan existir por el elevado número de Estados que previsiblemente serán parte de este Protocolo —y por la diversidad existente entre los distintos sistemas jurídicos—[39], se espera que el derecho interno ofrezca unos niveles mínimos de protección derivados de las obligaciones asumidas en virtud de otros tratados internacionales[40]. Entre otros, como parte de estas garantías y salvaguardias relacionadas con los derechos humanos y las libertades, se exige que se incluya el respeto del principio de proporcionalidad, al que ya nos hemos referido *supra*.

Asimismo, en la implementación de estos procedimientos de cooperación directa, se permite a los Estados parte introducir la exigencia de que sean supervisados por una autoridad judicial o por cualquier otra autoridad independiente. Esta condición adicional permitiría garantizar la protección de los derechos humanos y de las libertades que pueden verse afectados por la medida, y podría imponerse al regular la facultad de sus autoridades de emitir las solicitudes o requerimientos —como veremos, cuando se adapte la legislación nacional para cumplir con las obligaciones impuestas, respectivamente, en los arts. 6.1 y 7.1 del Segundo Protocolo—. Por último, siempre que no afecte a la buena administración de justicia —u a otros intereses públicos—, los Estados parte podrían considerar cómo repercuten estas medidas de cooperación directa sobre los derechos, las responsabilidades y los intereses legítimos de terceros; en concreto, en este caso, quienes pueden

39. Sobre el alcance del ámbito de aplicación territorial del Segundo Protocolo, *vid*., DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…, op. cit*., p. 126.

40. Entre otros, el Convenio Europeo de Derechos Humanos de 1950 —y sus Protocolos adicionales—, el Pacto internacional de derechos civiles y políticos de las Naciones Unidas de 1966, la Convención Americana sobre derechos Humanos de 1969 o la Carta Africana sobre Derechos Humanos y de los Pueblos de 1981 (Informe explicativo al Convenio sobre la Ciberdelincuencia, apartado 145).

verse afectadas son las propias entidades o los proveedores, entes de naturaleza privada —normalmente empresas—, a quienes se les pide la entrega de la información —derecho a la libertad de empresa, responsabilidades por revelar información, interés de no perder usuarios de su servicio…—[41].

5.2. La protección de los datos de carácter personal: una exigencia regulada con detalle en el art. 14 del Segundo Protocolo en defecto de otro acuerdo aplicable

Cuando se entrega la información solicitada en virtud de los procedimientos de cooperación directa que regula el Segundo Protocolo, se están transfiriendo datos de carácter personal —independientemente de que, como veremos, se trate de los menos sensibles o invasivos—; por ello, el art. 14 de este Protocolo regula las condiciones y salvaguardias relacionadas con la protección de los datos de carácter personal que habrán de respetarse. En principio, los apartados 2 a 15 de este detallado artículo son aplicables, sin embargo, la propia disposición prevé dos excepciones si los dos Estados parte implicados —el que pide los datos y aquel en cuyo territorio se encuentre la entidad o el proveedor—, bien están vinculados por un acuerdo internacional que ofrezca una regulación íntegra en materia de protección de datos para su transferencia en el marco de un proceso penal[42], bien no están vinculados por un acuerdo de tales características pero deciden mutuamente que la transferencia de datos en el marco de un proceso penal se realizará sujeta a determinadas normas internacionales —otros convenios, arreglos o acuerdos— distintas a las que detalla el art. 14.

Sin pretender realizar un análisis exhaustivo del art. 14, debe apuntarse que solo permite denegar la entrega de la información si ello se justifica en alguno de los motivos expresamente previstos por la normativa aplicable —sea el propio art. 14 o sean otros acuerdos internacionales—[43] o cuando existan pruebas de que el Estado parte que solicita los datos no respeta lo establecido en el art. 14[44]. En relación con aquello que puede afectar al proceso penal —y a las garantías que han de respetarse—, destaca el hecho de que no impide que, una vez recibidos los datos, el Estado parte aplique unas normas más estrictas para el tratamiento de estos por sus autoridades[45];

41. Sobre esto, *vid*., Informe explicativo al Convenio sobre la Ciberdelincuencia, apartado 148.
42. Sobre los tratados internacionales que podrían exceptuar la aplicación del art. 14, *vid*., BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit*., p. 13.
43. Art. 14.1.d) e Informe explicativo al Segundo Protocolo adicional, apartado 225.
44. Art. 15 e Informe explicativo al Segundo Protocolo adicional, apartados 282 a 287.
45. Art. 2.a) e Informe explicativo al Segundo Protocolo adicional, apartado 230.

además, es responsabilidad de los Estados parte que los datos se conserven con la debida calidad e integridad —lo que, como veremos, podría servir como base para exigirles poner a disposición del particular requerido vías para una transmisión segura—[46]; en el mismo sentido, son los Estados parte quienes han de contar con medios adecuados para la protección de los datos, garantizando que no sucedan incidentes —tales como su pérdida, acceso o revelación—[47]. También debe ponerse de relieve que el art. 14 no impida una posterior transferencia de los datos a otro Estado u organización internacional, aunque se requiere para ello el consentimiento expreso de la autoridad designada por el Estado parte en cuyo territorio se encuentra el particular que ha entregado los datos —entidad o proveedor—[48].

Finalmente, a efectos de garantizar la transparencia, se prevé la comunicación a la persona titular de los datos que se han entregado a otro Estado parte; esta notificación incluirá información como la base jurídica, los fines del tratamiento y el destinatario de los datos revelados. Se trata de una obligación que se impone al Estado parte, y no al particular que proporciona la información en la cooperación directa —si bien esto podría venirle impuesto por su propia política en la materia—, en todo caso —incluso si fuera aplicable a la entidad o al proveedor—, debemos señalar que el art. 14 también prevé que no se realice esta notificación si la autoridad emisora ha solicitado expresamente que se respete la confidencialidad, como se expone *infra*, esto podrá realizarse mediante la inclusión de lo que el Segundo Protocolo denomina "instrucciones procesales especiales".

IV. LA POSIBILIDAD DE SOLICITAR INFORMACIÓN SOBRE LOS REGISTRANTES DE NOMBRES DE DOMINIO A LAS ENTIDADES UBICADAS EN EL TERRITORIO DE OTRO ESTADO PARTE

1. FACULTAR A SUS AUTORIDADES Y PERMITIR A LAS ENTIDADES: LA DOBLE OBLIGACIÓN ASUMIDA POR LOS ESTADOS PARTE EN VIRTUD DEL ART. 6 DEL SEGUNDO PROTOCOLO

Centrándonos en el primer procedimiento de cooperación directa que introduce el Segundo Protocolo, bajo el título "Solicitud de información sobre el registro de nombres de dominio", el art. 6 impone una obligación

46. Art. 3 e Informe explicativo al Segundo Protocolo adicional, apartados 232 a 234.
47. Art. 7.a) e Informe explicativo al Segundo Protocolo adicional, apartados 246 a 248.
48. Art. 10.a) e Informe explicativo al Segundo Protocolo adicional, apartado 262.

doble a los Estados que lo ratifiquen. De un lado, les obliga a adoptar las medidas nacionales que sean necesarias a efectos de facultar a sus autoridades competentes para solicitar información a entidades que presten servicios de registro de nombres de dominio en el territorio de otro Estado parte; de otro lado, les obliga a permitir que las entidades de su territorio revelen la información del registrante de un nombre de dominio a las autoridades competentes de otro Estado parte.

A propósito de la segunda obligación que asumen los Estados parte en virtud del art. 6 del Segundo Protocolo, destaca el hecho de que, conforme a la redacción literal de su apartado segundo, es suficiente con que se eliminen los obstáculos que impidan a las entidades facilitar la información relativa a los registrantes, de modo que depende de cada Estado parte dotarla o no de carácter imperativo[49]. En consecuencia, el legislador nacional puede configurar el régimen de esta medida de dos modos distintos sin que ello tenga efectos sobre el principio de reciprocidad; puede hacerla preceptiva, de modo que, si la solicitud de la autoridad competente de otro Estado parte cumple los requisitos previstos en el art. 6.3 del Segundo Protocolo, la entidad deberá entregar la información, pudiendo ser sancionada si se niega al estar obligada a compartir los datos; o puede hacerla facultativa, con lo que, aun cuando se cumplan los requisitos y nada le impida proporcionar los datos, la decisión será tomada libremente por la propia entidad[50], que no podrá ser sancionada en caso de negativa al no estar obligada a ello.

En cualquiera de los dos supuestos anteriores —es decir, sea obligatorio o facultativo para la entidad proporcionar los datos requeridos conforme a su legislación nacional—, la solicitud emitida por la autoridad competente de otro Estado parte nunca podrá obligar a las entidades a facilitar la información, esto regirá al margen de cuales sean los efectos que la misma pudiera desplegar en el ordenamiento jurídico interno de quien la emite —por ejemplo, si en el Estado de emisión se trata de una orden de obligado

49. Sobre esta cuestión, *vid*., Informe explicativo al Segundo Protocolo adicional, apartado 83.

50. "Por tanto, son las entidades que prestan servicios de registro de nombres de dominio quienes han de determinar si divulgan la información solicitada, actuando dentro de los límites de las leyes aplicables de la jurisdicción a la que se someten" (traducción libre de la autora), SIRIUS Project, Cross-border Access to electronic Evidence, "Article 6 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Direct Requests for Domain Name Registration Information", last update: 23/01/2024, Eurojust — Europol, pág. 6 (disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/requests-for-domain-name-registration-information-under-article-6-of-the-second-additional-protocol-to-the-convention-on-cybercrime-23-01-2024.pdf, última consulta: 18 de abril de 2025).

cumplimiento para sus destinatarios—[51]. Ahora bien, cuando la entidad no coopere —y, de nuevo, independientemente del carácter obligatorio o facultativo de proporcionar los datos—, el Estado requirente podrá solicitarle que justifique su decisión de no revelar la información —pues así lo prevé el art. 6.5 del Segundo Protocolo—. Además, en tal caso, la respuesta que ofrezca la entidad no será definitiva, pues en principio podrán utilizarse otros instrumentos de cooperación y asistencia mutua —ahora sí, entre autoridades estatales competentes— para obtener esos datos.

2. LAS ENTIDADES QUE PRESTAN SERVICIOS DE REGISTRO DE NOMBRES DE DOMINIO COMO RECEPTORAS DE LA SOLICITUD Y SU CONDICIÓN DE PRESTADORES DE SERVICIOS

La receptora de la solicitud de cooperación directa será siempre una "entidad que preste servicios de registro de nombres de dominio". Es interesante apuntar que tales entidades son catalogadas por el Reglamento de Prueba Electrónica de la Unión Europea[52], en su art. 3.3), como una categoría de prestador de servicios[53] —sin diferenciar su régimen del de otros prestadores, como, por ejemplo, los que prestan servicios de direcciones IP o servicios de comunicaciones electrónicas—[54]. Sin embargo, el Segundo Protocolo parece excluir a quienes prestan servicios de nombres de dominio de este concepto más amplio, evitando en todo momento utilizar la expresión prestadores o proveedores de servicios en el art. 6, estableciendo un régimen propio para estas entidades y regulándolas como algo distinto a los proveedores de servicios de quienes se ocupa, como veremos, en su

51. Así lo establece el Informe explicativo al Segundo Protocolo adicional en su apartado 77. En esta línea, BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 6, quien afirma "Cumplidos estos presupuestos, todo conduce a que las entidades revelen la información de dominio, pero el texto del precepto no presupone una obligación automática de transmisión de la información".
52. Reglamento (UE) 2023/1543, de 12 de julio de 2023.
53. Sobre las tres categorías de prestadores de servicios que pueden ser destinatarios de las órdenes europeas de producción o de conservación conforme al Reglamento de Prueba Electrónica, *vid.*, LLOPIS NADAL, P. "La cooperación judicial penal con el entorno digital como escenario: los prestadores de servicios como coprotagonistas del Reglamento 2023/1543 sobre las órdenes europeas de producción y de conservación a efectos de prueba electrónica", en CASTELLÓ PASTOR, J. J., *Análisis del Reglamento (UE) de Servicios Digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 452 y 453.
54. En este sentido, SIRIUS Project, Cross-border Access to electronic Evidence, "Article 6 of the Second Additional Protocol…", pág. 2 y nota de pág. 12.

art. 7. En esta línea, el art. 1.c) del Convenio ya ofrecía una definición de proveedor de servicios limitada y en la que no se incluían las entidades que prestan servicios de registro de nombres de dominio.

A propósito de las entidades con las que podrá llevarse a cabo la cooperación directa prevista en el art. 6, el texto del Segundo Protocolo no matiza nada más, pero sí lo hace, en cambio, su Informe explicativo, al apuntar que forman parte de estas tanto los *registradores* como los *registros*, sin limitar a estos dos sujetos las entidades a quienes puede solicitarse la información. Así, *registradores* es la denominación que reciben las "organizaciones que venden nombres de dominio al público", mientras que por *registros* se entiende los "operadores de registros regionales o nacionales que mantienen bases de datos autorizadas (…) de todos los nombres de dominio registrados para un nivel de dominio superior y aceptan solicitudes de registro"[55].

3. LOS DATOS QUE PUEDEN SOLICITARSE A LAS ENTIDADES QUE PRESTAN SERVICIOS DE REGISTRO DE NOMBRES DE DOMINIO: RELEVANCIA Y REQUISITOS

Los datos que pueden solicitarse y obtenerse de las entidades que prestan servicios de registro de nombres de dominio son particularmente relevantes al inicio de toda investigación penal y servirán como base para posteriores solicitudes de prueba electrónica —y, en su caso, de nuevos procedimientos de cooperación, directa o internacional—[56]. No obstante, la información que puede recabarse se encuentra doblemente delimitada por el art. 6 del Segundo Protocolo al exigir que concurran, de manera acumulativa, dos requisitos. Primero, ha de ser información que, en el momento de la solicitud, ya esté en poder de la entidad o se encuentre bajo su control, no pudiendo exigírsele que la obtenga *ex post* a raíz de la petición efectuada por la autoridad de otro Estado parte. SIRIUS Project, en su análisis de este nuevo procedimiento de cooperación directa, interpreta que las expresiones *en su poder* o *bajo su control* "hacen referencia tanto a una posesión física de la información, como a situaciones en las que la entidad no posee físicamente la información, sino que esta se encuentra almacenada de manera remota, pero bajo el control de la propia entidad"[57].

El segundo requisito que el art. 6 impone a los datos que pueden solicitarse es que la finalidad de la información requerida debe ser, exclusivamente, la de

55. Informe explicativo al Segundo Protocolo adicional, apartado 75.
56. En esta línea, Informe explicativo al Segundo Protocolo adicional, apartado 73.
57. Traducción libre de la autora, SIRIUS Project, Cross-border Access to electronic Evidence, "Article 6 of the Second Additional Protocol…" pág. 3.

hallar al registrante de un nombre de dominio o la de ponerse en contacto con él. Esto es, ha de tratarse de datos que posibiliten conocer la identidad de la persona física o jurídica titular registral de un dominio de internet —nombre y apellidos, denominación, números de identificación— u obtener información adicional de quien ha registrado un dominio que permita comunicarse con él —su número de teléfono, su dirección postal o su correo electrónico—, siendo posible pedir en la misma solicitud alguno, algunos o todos estos datos a condición de que se justifique su necesidad y pertinencia.

4. LOS REQUISITOS QUE HA DE CUMPLIR LA SOLICITUD Y EL NECESARIO RESPETO DE LAS GARANTÍAS PROCESALES EN LA ENTREGA DE LA INFORMACIÓN

Aun cuando el propósito de la cooperación directa que regula el art. 6 del Segundo Protocolo es facilitar la entrega de datos originados en el entorno digital, su solicitud a la entidad que presta servicios de registro de nombres de dominio deberá realizarse por medios analógicos a no ser que, la propia requerida, acepte su presentación en formato electrónico. En la medida en que el ámbito de actuación de estas entidades es el entorno digital, es previsible que estén dispuestas a recibir solicitudes haciendo uso del correo electrónico o de otras vías de contacto habilitadas por la misma.

La solicitud que se remite a la entidad habrá de contener, necesariamente, unos elementos mínimos que se detallan en el art. 6.3. Como se ha apuntado, si bien la información que se puede requerir es limitada, en la solicitud es posible pedir distintos datos relativos al titular del dominio registrado —nombre y apellidos, número de teléfono, dirección postal, correo electrónico…—, debiendo detallarse todos ellos. Se exige, asimismo, que la autoridad requirente incluya una declaración justificando que la petición de los datos se realiza con arreglo al Segundo Protocolo y, en ese sentido, confirmar que es necesaria y pertinente en el marco de un proceso penal específico y que solo se utilizará con tal fin —respetando, de ese modo, los principios de especialidad y de proporcionalidad a los que nos hemos referido *supra*—. Ahora bien, a diferencia de lo que prevé el art. 7, entre el contenido mínimo de la solicitud no se prevé incluir referencias al delito o delitos objeto del proceso penal ni a las disposiciones legales aplicables —siendo suficiente con afirmar que su solicitud se realiza en el marco de un proceso penal—, por lo que la entidad requerida, un ente de naturaleza privada, podría tener que decidir sobre la entrega de datos en un procedimiento de cooperación directa sin conocer los hechos delictivos que han dado lugar a la causa penal y sin conocer los fundamentos jurídicos esenciales del asunto.

Es la autoridad que solicita la información quien determina, en su propia solicitud, el plazo en que habrán de entregarse los datos y la forma en que se realizará la entrega. Sobre el plazo, será el derecho interno de la autoridad emisora el que lo establezca, algo que deberá realizarse teniendo en cuenta que la cooperación directa se introduce con la finalidad de lograr un intercambio de información más eficiente —y más rápido— que el que se realiza con la cooperación internacional; podría servir como paradigma el derecho de la Unión Europea que, como regla general, prevé la entrega de los datos lo antes posible y, a más tardar, en un plazo de diez días[58]. Sobre la forma, el art. 6.4 *in fine* prevé que puedan exigirse, adicionalmente, niveles adecuados de seguridad y de autenticación; siendo esto fundamental para garantizar la integridad de los datos en el marco de un proceso penal, debería ser el propio Estado que requiere la información a un ente de naturaleza privada quien habilitara los instrumentos necesarios para que la transmisión de datos se realizara con todas las garantías, indicando a la entidad que esa vía ha de ser la forma de entregarlos.

Por último, en cuanto al contenido de la solicitud, el Segundo Protocolo deja abierta la posibilidad de que la autoridad incluya "cualesquiera otras instrucciones procesales especiales". La instrucción procesal que cabe esperar es la del respeto de la confidencialidad, en especial, el no poner en conocimiento del titular del registro —ni de terceros—, el hecho de que, en el marco de un proceso penal que se desarrolla en otro Estado, se ha recibido una solicitud para la entrega de datos que permitan identificar o contactar con quien ha registrado un dominio, ni el hecho de que, efectivamente, se ha transmitido la información a la autoridad requirente. El Informe explicativo hace referencia a la petición de confidencialidad, recordando la importancia de conocer de antemano tanto el derecho interno del Estado parte donde se encuentra la entidad, como la política de la propia entidad requerida, pues existen notables diferencias en el modo de abordar esta cuestión. En cualquier caso, no debe olvidarse que el uso de estas pruebas electrónicas en el marco de un proceso penal habrá de realizarse con pleno respeto de las garantías y de los derechos de la defensa, por lo que, siempre que sea posible, deberá informarse al titular de los datos sin demora o proporcionarle vías de recurso efectivas[59].

---

58. Reglamento de Prueba Electrónica, art. 10.

59. A este propósito, destaca el art. 13 del Reglamento de Prueba Electrónica destinado, íntegramente, a regular todo lo relativo a la información al usuario y a la confidencialidad; la referida disposición impone la obligación de informar sin demora indebida a la persona cuyos datos se han solicitado y delimita los supuestos en que, excepcionalmente, sería posible demorar, restringir u omitir tal comunicación. Sobre

V. LA POSIBILIDAD DE SOLICITAR INFORMACIÓN SOBRE LOS ABONADOS A LOS PROVEEDORES DE SERVICIOS QUE SE ENCUENTRAN EN EL TERRITORIO DE OTRO ESTADO PARTE

1. LAS OBLIGACIONES ASUMIDAS EN VIRTUD DEL ART. 7 DEL SEGUNDO PROTOCOLO Y LA POSIBILIDAD DE RESERVARSE EL DERECHO A NO APLICARLO DE MANERA TOTAL O DE MANERA PARCIAL

1.1. La doble obligación que impone del art. 7 del Segundo Protocolo y la posibilidad de restringir las autoridades competentes de los otros Estados parte

El art. 7 del Segundo Protocolo regula con detalle el procedimiento de cooperación directa que tiene como objetivo la revelación de información relativa a los abonados; en virtud de este, e igual que con el primer procedimiento —expuesto *supra*—, los Estados parte asumen una doble obligación. De un lado, quedan obligados a adoptar las medidas nacionales que sean necesarias a efectos de facultar a sus autoridades competentes para dictar requerimientos dirigidos a los proveedores de servicios ubicados en el territorio de otro Estado parte pidiéndoles la entrega de información sobre sus abonados; de otro lado, quedan obligados a permitir que los proveedores de servicios que estén en su territorio revelen la información relativa a sus abonados a las autoridades competentes de otro Estado parte[60].

Del mismo modo que sucedía respecto de las entidades que prestan servicios de registros de nombres de dominio, la segunda obligación de adoptar medidas legislativas ha de considerarse cumplida si el Estado elimina los obstáculos que impiden a los proveedores de servicios facilitar a las autoridades de otro Estado parte la información relativa a sus abonados. Por tanto, dependerá del legislador nacional conceder carácter preceptivo o facultativo a esta medida, sin que ello tenga efectos sobre el principio de reciprocidad; en consecuencia, podrán coexistir en los diferentes Estados

---

la confidencialidad como una limitación o condición de uso de los datos obtenidos en aplicación del Segundo Protocolo, *vid*., GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., "El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad", *op. cit*., p. 26.

60. "Con ello [la obligación introducida por el art. 7.2] se consigue una regulación legal efectiva respecto de actuaciones que ya se estaba realizando por parte de algunos países, pero que precisaban de un tratamiento legislativo más detallado para su aceptación por otros Estados" [TEJADA DE LA FUENTE, E., Entrevista — Ciberderecho, *op. cit*., p. 4].

parte regímenes en los que sea obligatorio para los proveedores facilitar la información si se cumplen todos los requisitos, con regímenes en que los proveedores tengan permitido entregarla en caso de que se cumplan los requisitos, pero sin estar obligados a ello, y correspondiéndoles en última instancia la decisión[61].

Sí supone una notable diferencia respecto de lo previsto en el art. 6 el hecho de que, en el procedimiento de cooperación directa consistente en la revelación de información relativa a los abonados, los Estados parte estén facultados para limitar las autoridades competentes que pueden requerir tal información a los proveedores de servicios de su territorio. En concreto, pueden exigir que solo las autoridades judiciales o la fiscalía de un Estado —o, en su caso, miembros de otros entes actuando bajo su supervisión o bajo una supervisión independiente—, emitan los requerimientos que regula el art. 7 e inicien este procedimiento de cooperación directa con los proveedores de servicios. De este modo, se permite a los Estados parte restringir el amplio concepto de autoridad competente previsto en el art. 3.2.b) del Segundo Protocolo —y que ha sido expuesto *supra*—; no obstante, esto deberá realizarse necesariamente con carácter general, mediante una declaración que habrá de ser formulada por el Estado parte en el momento de la firma del Protocolo o cuando se deposite su instrumento de ratificación, aprobación o aceptación; asimismo, realizada la declaración, no será posible que el Estado parte —ni sus proveedores de servicios— se nieguen a aceptar requerimientos que procedan de alguna de estas autoridades[62].

1.2. La posibilidad de realizar reservas de distinta extensión para la no aplicación del art. 7 por un Estado parte del Segundo Protocolo

Si bien las dos obligaciones expuestas en el apartado inmediatamente anterior deben respetarse por todos los Estados parte del Segundo Protocolo, el art. 7.9 permite que en el momento de su firma o del depósito de su instrumento de ratificación, aceptación o aprobación, el Estado pueda realizar reservas de distinto alcance relativas al procedimiento de cooperación directa para la entrega de datos de los abonados. A propósito de las posibilidades que ofrece el Segundo Protocolo de realizar declaraciones y reservas, DE HOYOS SANCHO destaca que estas se introducen "a fin de que […] pueda incorporarse a los distintos sistemas jurídicos en que se tendrá

61. Sobre esta cuestión, *vid.*, Informe explicativo al Segundo Protocolo adicional, apartado 100.

62. SIRIUS Project, Cross-border Access to electronic Evidence, "Article 7 of the Second Additional Protocol…", pág. 5.

que aplicar" y que "le dotará de la flexibilidad que necesita un texto llamado a ser aplicado en decenas de países con notables diferencias entre sí"[63].

La reserva de mayor extensión es la que permite el art. 7.9.a), consistente en la posibilidad de reservarse el derecho a no aplicar el art. 7 del Segundo Protocolo en toda su integridad[64]. Como es lógico, el Estado parte que haga uso de esta reserva no deberá cumplir con las dos obligaciones descritas; por tanto, no habrá de adoptar medidas para permitir a los proveedores de servicios de su territorio revelar información sobre sus abonados a autoridades competentes de otro Estado parte; y tampoco, sobre la base del principio de reciprocidad, habrá de adoptar medidas para facultar a sus propias autoridades a requerir tal información a prestadores de servicios ubicados en el territorio de otro Estado parte, pues la reserva trae como consecuencia que no estará autorizado para emitir tales requerimientos[65]. Para el caso de que haya Estados parte del Segundo Protocolo que opten por reservarse el derecho a no aplicar este procedimiento de cooperación directa con los proveedores de servicios, queda la posibilidad de obtener la información relativa a los abonados recurriendo a la cooperación internacional entre autoridades estatales que se regula en el art. 8 —el cual, además de para solicitar datos de los abonados puede utilizarse para solicitar datos de tráfico—[66].

La reserva de menor extensión se regula en el art. 7.9.b) e implica la posibilidad de excluir determinados datos de los abonados de la información que puede revelarse en aplicación del art. 7. La razón de ser de esta acotada reserva reside en el hecho de que, la información relativa a los abonados comprende diferentes tipos de datos que, en principio, deben facilitarse a

63. DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…*, *op. cit.*, p. 133. Concluye la autora que, hasta que no se conozcan tales declaraciones y reservas, "no podremos valorar toda la operatividad de las nuevas herramientas de cooperación internacional que se contienen en el Segundo Protocolo".

64. En la fecha en que se redactó este capítulo, Japón —uno de los Estados que habían ratificado el Segundo Protocolo—, era el único que se había reservado el derecho a no aplicar el art. 7, en su integridad, sobre la base de la facultad concedida por el art. 7.9.a). Reservation contained in a letter from the Consul General of Japan in Strasbourg, dated 10 August 2023, deposited with the instrument of acceptance on 10 August 2023 (disponible en: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=224&codeNature=0, última consulta, 18 de abril de 2025).

65. Informe explicativo al Segundo Protocolo adicional, apartado 122.

66. "La causa de que las solicitudes de información sobre los abonados se encuentren en dos preceptos diferentes se debe a que hay Estados firmantes de la Convención que no admiten la cooperación directa con proveedores de servicios […]" [TEJADA DE LA FUENTE, E., Entrevista — Ciberderecho, *op. cit.*, p. 4].

la autoridad competente de otro Estado parte —el alcance de los mismos se detalla *infra*—; sin embargo, el derecho interno puede categorizar estos datos de manera diferente, de modo que, lo que a los efectos del Segundo Protocolo constituye simplemente datos de abonados, en algunos Estados parte recibe la calificación de datos de tráfico —y, por ello, son considerados más sensibles—. Esto sucederá, en concreto, cuando se pide la entrega de los números que configuran la dirección IP desde la que ha actuado el abonado[67], por este motivo, se permite a quienes son parte del Segundo Protocolo reservarse el derecho a no aplicar el art. 7 a "la revelación de determinados números de acceso"[68]. Del mismo modo que sucedía con la reserva general, el principio de reciprocidad determina que el Estado parte que hace uso de esta reserva parcial no estará autorizado para emitir requerimientos solicitando a proveedores de servicios ubicados en el territorio de otro Estado parte la revelación de datos que impliquen las categorías de números de acceso contenidas en su reserva[69].

2. LOS PROVEEDORES DE SERVICIOS DEFINIDOS EN EL CONVENIO DE BUDAPEST COMO RECEPTORES DEL REQUERIMIENTO

Los receptores del requerimiento de cooperación directa serán siempre los proveedores de servicios; sin embargo, a pesar de su relevante papel en estos procedimientos, el Segundo Protocolo, en su art. 3.1, nos remite a lo previsto en el Convenio de 2001, por lo que se ha perdido la oportunidad de ofrecer una definición actualizada —o, al menos, adaptada a la terminología que ha surgido en las dos últimas décadas—. A partir del art. 1.c) del Convenio, junto a su Informe explicativo[70], es posible concluir que por proveedor de servicios cabe entender toda entidad que permita a sus usuarios comunicarse entre sí por medio de un sistema informático —siendo irrelevante que sea pública o privada, gratuita o de pago—, así como toda

67. La propia Unión Europea afirma "las direcciones IP deben considerarse datos personales y gozar de plena protección […] en materia de protección de datos. Además, en determinadas circunstancias, las direcciones IP pueden considerarse datos de tráfico. Asimismo, los números de acceso […] se consideran datos de tráfico en algunos Estados miembros. No obstante, a efectos de una investigación penal específica, las autoridades policiales pueden solicitar una dirección IP, así como números de acceso […] con el único fin de identificar al usuario […]. En tales casos, procede aplicar el mismo régimen que a los datos de los abonados" (Reglamento de Prueba Electrónica, considerando 32).
68. Informe explicativo al Segundo Protocolo adicional, apartado 93.
69. Informe explicativo al Segundo Protocolo adicional, apartado 122.
70. Informe explicativo al Convenio sobre la Ciberdelincuencia, apartados 26 y 27.

entidad cuya función sea procesar o almacenar datos informáticos en nombre del servicio de comunicación o de los usuarios —lo que incluye a quienes ofrecen conexión a internet y a los alojadores de contenidos, entre los que encontramos a las actuales plataformas digitales—; se trata, por tanto, de un concepto menos amplio que el previsto en el art. 3.3 del Reglamento de Prueba Electrónica de la Unión Europea bajo la denominación de prestadores de servicios[71]. Determinar los proveedores de servicios que podrán ser receptores del requerimiento es importante pues repercute sobre los datos que abarca la información relativa a los abonados.

Se exige, adicionalmente, que el proveedor de servicios se encuentre en el territorio de otro Estado parte. Como ya se ha apuntado, el art. 18.1 del Convenio introdujo una medida similar, pero limitada al ámbito interno; el art. 7 del Segundo Protocolo da un paso más y regula la cooperación directa con los proveedores ubicados en otros Estados. A este propósito, el Informe explicativo insiste en que el proveedor de servicios "deberá estar físicamente presente en la otra Parte", no siendo suficiente para entender que se encuentra en el territorio de ese Estado cuando "haya establecido una relación contractual con una empresa de una Parte (…) pero no esté físicamente presente"[72]. Esto ha de llevarnos a excluir la posibilidad de que Estados no miembros de la Unión Europea consideren que el proveedor se encuentra en el territorio de un Estado miembro de la Unión por el mero hecho de que ha designado aquí un establecimiento o un representante legal a efectos de cumplir con la exigencia que le impone el Reglamento de Prueba Electrónica de la Unión Europea —y, en concreto, por la Directiva[73] que lo acompaña—[74].

3. LA DELIMITACIÓN DE LOS DATOS RELATIVOS A LOS ABONADOS QUE PUEDEN SOLICITARSE A LOS PROVEEDORES DE SERVICIOS

El acceso a la información relativa al abonado que utiliza determinado servicio es particularmente relevante en el entorno digital, no en vano, el

71. SIRIUS Project, Cross-border Access to electronic Evidence, "Article 7 of the Second Additional Protocol…", pág. 3 y nota de pág. 13.
72. Informe explicativo al Segundo Protocolo adicional, apartado 99.
73. Directiva 2023/1544, de 12 de julio de 2023.
74. Sobre esta obligación impuesta a los prestadores que ofrecen sus servicios en el territorio de la Unión Europea, *vid*., DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…*, *op. cit.*, pp. 117 a 124; LLOPIS NADAL, P. "La cooperación judicial penal con el entorno digital como escenario…", *op. cit.*, pp. 455 a 457.

Informe explicativo al Segundo Protocolo destaca que se trata de la información solicitada con más frecuencia en las investigaciones penales sobre ciberdelincuencia o en las que se precisan pruebas electrónicas[75]. Respecto de los datos que pueden solicitarse a los proveedores de servicios, el art. 7 exige que se trate de "información específica almacenada relativa a los abonados, que obre en poder o esté bajo el control de dicho proveedor de servicios". En consecuencia, la autoridad que requiere los datos deberá concretarlos, esto es, determinar exactamente qué información precisa, sin que se permita solicitar y entregar datos de manera generalizada e indiscriminada[76]. Además, no podrá exigirse la obtención de tales datos tras la recepción del requerimiento, sino que el proveedor deberá de tenerlos ya registrados en sus bases de datos o alojados en sus servidores, reiterándose la idea de posesión física de la información y de control de datos almacenados remotamente que ha sido expuesta *supra* a propósito del art. 6[77].

No menciona nada más el art. 7 a propósito de cuáles son esos datos, por ello debemos remitirnos de nuevo a las definiciones del Convenio, en esta ocasión a las previstas en el art. 18, cuyo apartado tercero delimita el concepto *datos relativos a los abonados* estableciendo sus características[78]. En primer lugar, permite que se trate de información que se presente bajo la forma de datos informáticos —esto es, en formato digital— o en cualquier otra forma —admitiéndose, por tanto, la que está en formato analógico[79]—. En segundo lugar, se excluyen expresamente los datos sobre el tráfico y los datos sobre el contenido[80], esto es, aquellos considerados más sensibles y que permiten

75. Informe explicativo al Segundo Protocolo adicional, apartado 92.
76. Las disposiciones del Segundo Protocolo "no pueden utilizarse para la producción masiva o a granel de datos" (Informe explicativo al Segundo Protocolo adicional, apartado 97).
77. En este sentido, SIRIUS Project, Cross-border Access to electronic Evidence, "Article 7 of the Second Additional Protocol…", pág. 3.
78. Es interesante, de antemano, detenernos en la extensión del concepto *abonado* utilizado en el art. 18.3 del Convenio, pues su Informe explicativo considera que "abarca a una amplia gama de clientes del proveedor", siendo indiferente si "tienen abonos pago", "pagan en función del uso que hacen" o "reciben los servicios en forma gratuita", y añade la posibilidad de facilitar "información respecto de las personas que tienen derecho a utilizar la cuenta del abonado" (Informe explicativo al Convenio sobre la Ciberdelincuencia, apartado 177).
79. Sería el caso, por ejemplo, de la información de un abonado a los servicios que presta el proveedor requerido que pueda extraerse a partir de un contrato firmado en papel.
80. Para una definición de ambas categorías nos remitimos a lo expuesto *supra*, en la exposición del art. 18 del Convenio, asimismo, debemos añadir que el Segundo Protocolo ha desaprovechado la oportunidad de actualizar el concepto de *datos de tráfico* y de introducir una definición de *datos de contenido*.

conocer aspectos de la vida privada de las personas; ahora bien, los datos sobre el tráfico podrán obtenerse mediante el procedimiento de cooperación internacional que regula el art. 8 del Segundo Protocolo[81]. Y, en tercer lugar, se exige que sea información relacionada con los abonados al servicio que presta el proveedor requerido y a partir de la cual se puedan determinar aspectos sobre el servicio utilizado —por ejemplo, tipo o tiempo de la prestación—; sobre el propio abonado, lo que incluye no solo su identidad, dirección y número de teléfono, sino también los números de acceso —si bien, como se ha apuntado, esto podría ser objeto de reserva—, e, incluso, los datos de facturación y de pago que consten en el contrato celebrado entre ambas partes; así como sobre el lugar donde se encuentran los equipos de comunicaciones utilizados —sin que esto se confunda con los datos de tráfico—[82].

4. EL CONTENIDO MÍNIMO DEL REQUERIMIENTO Y LA POSIBILIDAD DE ACOMPAÑARLO DE INFORMACIÓN COMPLEMENTARIA

Del mismo modo que sucedía con la solicitud de información dirigida a las entidades que prestan servicios de registro de nombres de dominio, este requerimiento deberá presentarse por medios analógicos, salvo que el proveedor de servicios requerido acepte su presentación en formato electrónico. Si bien es lógico esperar que esto sea así, dado que el medio en el que estos sujetos desarrollan sus funciones es el entorno digital, destaca el hecho de que ello no pueda imponerse por el Estado parte cuando adopte las medidas legislativas necesarias para permitir a los proveedores que se encuentran en su territorio facilitar la información. Además, también para este procedimiento de cooperación directa pueden exigirse niveles adecuados de seguridad y de autenticación, como ya se ha apuntado respecto de la primera medida, esto es esencial para garantizar la integridad de los datos en

81. Apunta CERRATO GURI que para la solicitud de datos de alguna de estas dos categorías "deberá activarse el procedimiento del art. 8 del Protocolo, que no se conforma con la comunicación directa entre autoridad y prestador del servicio, por el mayor grado de injerencia que supone en la intimidad de su titular y de otras personas que hayan podido intervenir en las comunicaciones. Así, en estos casos […] se opta por la comunicación entre partes para que sea la receptora de la orden la que compela al prestador de servicios de su territorio a presentar la información sobre su abonado o datos relativos al tráfico" [CERRATO GURI, E., "Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de prueba electrónica", *Revista General de Derecho Europeo*, núm. 61 (2023), pp. 175 y 176.

82. Para un mayor detalle sobre esto, *vid*., Informe explicativo al Convenio sobre la Ciberdelincuencia, apartados 177 a 183.

el marco de un proceso penal, por lo que Estado que emite el requerimiento debería ofrecer al particular vías adecuadas para que la transmisión de datos se realice con todas las garantías.

Con mayor detalle que la solicitud para poner en funcionamiento el primer procedimiento de cooperación directa, el art. 7 del Segundo Protocolo regula en dos instancias el contenido del requerimiento por el que se pide la entrega de datos relativos a los abonados. Así, en su apartado tercero concreta la información mínima que la solicitud deberá contener, mientras que en el apartado cuarto detalla la información complementaria que podría incluirse.

4.1. El contenido mínimo del requerimiento por el que se solicita a los proveedores de servicios información relativa a sus abonados

En cuanto al contenido mínimo, además de la identificación de la autoridad emisora del requerimiento y del proveedor de servicios receptor de este, se prevé que también se identifique a la autoridad que necesita la información requerida en el caso de que no coincida con la primera. Lo anterior sucederá cuando, con base en el art. 7.2.b), el Estado parte en cuyo territorio se encuentra el proveedor haya formulado la declaración consistente en restringir las autoridades que pueden remitir tal requerimiento; en el resto de los casos, tratándose de información solicitada en el marco de un proceso penal específico, la autoridad que precisa los datos habrá de ser, necesariamente, una de las autoridades competentes para emitir el requerimiento conforme al art. 3.b) —ahora bien, como ejemplo de una situación en que sea diferente la autoridad emisora y la autoridad que necesita los datos, el Informe explicativo se refiere al caso en que solo la autoridad judicial puede emitir el requerimiento, pero los datos son requeridos por fiscales u otros investigadores en el marco de una causa penal[83]—.

Entre este contenido mínimo del requerimiento también se exige una declaración por la que se justifique que la información se solicita con arreglo al Segundo Protocolo —respetándose, por tanto, los principios de especialidad y de proporcionalidad, expuestos *supra*—, esta deberá ir acompañada de la referencia al delito o delitos objeto del proceso penal para el que se requieren los datos —algo que no se exige en la solicitud que regula el art. 6—. Y, por último, es necesario detallar la información específica que se solicita, respetándose los límites expuestos en el apartado precedente a propósito de los datos que es posible requerir.

83. Informe explicativo al Segundo Protocolo adicional, apartado 103.

4.2. La información complementaria al requerimiento y la necesidad de mayor claridad sobre cómo, quién, cuándo y qué habrá de aportarse

Respecto de la información complementaria, el art. 7.4 se limita a mencionar que el requerimiento "irá acompañado de la información complementaria siguiente", pasando a enumerar hasta un total de ocho ítems; el Informe explicativo, por su parte, aclara que, con frecuencia, lo solicitado en el requerimiento solo puede ejecutarse si se recibe información complementaria[84]. De antemano, debemos indicar que, si bien la forma verbal denota que es obligatorio adjuntar tal información ("irá")[85], su carácter de "complementaria" podría llevar a pensar que esta no ha de exigirse necesariamente en todos los supuestos; en consecuencia, entendemos que es oportuno señalar varias cuestiones sobre este contenido adicional.

En primer lugar, no queda claro si esta información complementaria se proporcionará de oficio por la autoridad que emite el requerimiento atendiendo a las circunstancias del caso concreto —es decir, no con carácter general—, o, en cambio, si es el Estado parte en cuyo territorio se encuentra el proveedor de servicios quien puede exigir que se incluya tal información —algo que no podrá hacer con carácter general y que, si decide hacer de antemano, por ejemplo, al adoptar las medidas legislativas para cumplir con la obligación que le impone el art. 7.2.a), deberá acotar a determinadas situaciones—; esto último, como veremos, es lo que parece desprenderse del art. 7.5.a) en aquellos casos en que exige ser notificado simultáneamente. En segundo lugar, no se precisa en qué momento habrá de proporcionarse esa información, si junto al mismo requerimiento —lo que será necesario cuando se imponga por el Estado parte en cuyo territorio se encuentra el proveedor requerido—, o si en un momento posterior —bien de oficio, bien, como parece más lógico, a instancia del proveedor de servicios o de la autoridad del Estado parte donde este se encuentra—. En tercer y último lugar, también sería necesario concretar si se ha de aportar todos los elementos enumerados en el art. 7.4 o si cabe la posibilidad de exigir —o de presentar— tan solo alguno/s de ellos, según las circunstancias del caso.

A pesar de lo defendido, destaca el hecho de que entre la información complementaria se prevean ítems que han de formar parte del contenido mínimo de la solicitud dirigida a las entidades que prestan servicios de registro de nombres de dominio, este es el caso del plazo y la forma en que debe enviarse la información y la previsión de instrucciones procesales espe-

84. Informe explicativo al Segundo Protocolo adicional, apartado 105.

85. BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 6, también califica esta información como obligatoria.

ciales. Para la explicación y análisis de los plazos y la forma nos remitimos a lo que se ha expuesto *supra*, a propósito del procedimiento de cooperación directa regulado en el art. 6, al entender que se da identidad total en su aplicación a ambas medidas —si bien sobre el plazo para que los proveedores de servicios ofrezcan una respuesta a la autoridad que requiere los datos debemos apuntar la necesidad de tener en cuenta la previsión del art. 7.8 del Segundo Protocolo, que es expuesta *infra*, la cual parece indicarnos que todo plazo prudencial deberá ser de al menos treinta días[86]—.

En cuanto a las instrucciones procesales especiales, del mismo modo que con la primera medida de cooperación directa, también entre estas será posible incluir una solicitud de confidencialidad; ahora bien, como nos recuerda el Informe explicativo, respetar el carácter confidencial de la medida no podrá tener como consecuencia impedir que el proveedor de servicios consulte con la autoridad del Estado parte en cuyo territorio se encuentra si esta ha hecho uso de la facultad que le atribuye el art. 7.5 —y que se explica con detalle *infra*—[87]. Más allá de esto, destaca que como parte de esta información complementaria sí se incluyan referencias tanto a la base legal que habilita a la autoridad emisora a presentar el requerimiento, como a las normas —y sanciones— aplicables al delito que fundamenta la solicitud.

Adicionalmente, entre la información complementaria se prevé la posibilidad de incluir el contacto de la autoridad a la que deben enviarse los datos y a la que se le podrá pedir más información; sin embargo, no está clara la autoridad a la que se refiere el art. 7.4.c) —y que luego es mencionada en varias ocasiones en el art. 7.5—, esto es, si se trata de la autoridad emisora, si se refiere a la autoridad que necesita la información cuando ambas no coincidan —por ejemplo, por haber introducido el Estado parte del territorio donde se encuentra el proveedor de servicios la exigencia permitida por el art. 7.2.b)— o si es una tercera autoridad responsable de centralizar todas las cuestiones relativas a los requerimientos que se emitan con base en este procedimiento de cooperación directa. Por último, la norma incluye hacer referencia a si se ha solicitado la conservación de los datos requeridos, junto a toda la información al respecto —por ejemplo, la fecha en que se pidió—, ahora bien, el Segundo Protocolo no regula nada a propósito de la conservación de los datos, por lo que esta solicitud se habrá realizado con base en

86. En este sentido, BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest…", *op. cit.*, p. 7, quien sostiene "Se prevé un plazo general de 30 días para que el proveedor revele la información (que podrá ser ampliado en la 'información complementaria' que se remite con la solicitud)".

87. Informe explicativo al Segundo Protocolo adicional, apartado 106.

las medidas nacionales adoptadas para cumplir con las obligaciones que impone el Convenio a los Estados parte —en especial, en sus arts. 16 y 29—.

Del mismo modo que sucedía con el primer procedimiento de cooperación directa, en relación con el requerimiento dirigido a los proveedores de servicios para la entrega de datos relativos a sus abonados destaca que ni la información mínima, ni la información complementaria, incluyan los hechos que han dado lugar a la causa penal —o, al menos, un breve resumen de estos—. La mencionada omisión, completamente lógica dada la naturaleza privada del receptor del requerimiento, puede conducir a que el proveedor de servicios decida sobre la entrega —y, con ello, afecte a derechos fundamentales— sin poder valorar con integridad todas las circunstancias; esto se soluciona parcialmente en la segunda medida por la posibilidad de que, cuando la autoridad del Estado parte requerido es notificada o consultada, esta pueda solicitar y obtener de la autoridad emisora del requerimiento un resumen de los hechos relacionados con el proceso penal —esto se expone con detalle *infra*—.

5. LA POSIBLE INTERVENCIÓN DEL ESTADO PARTE EN CUYO TERRITORIO SE ENCUENTRA EL PROVEEDOR DE SERVICIOS CON CARÁCTER PREVIO A FACILITAR LA INFORMACIÓN

La cooperación directa para la entrega de información sobre el registro de nombres de dominio se lleva a cabo sin que haya intervención alguna del Estado parte del territorio donde se encuentra la entidad; en cambio, en la cooperación directa con los proveedores de servicios para obtener información de los abonados se prevé la posibilidad de que el Estado parte del territorio donde se encuentra el particular requerido intervenga. Esta intervención podrá realizarse de dos modos distintos, quedando, en cualquier caso, sujeta a lo que voluntariamente decida cada Estado parte.

5.1. La posibilidad de que el Estado parte exija notificación simultánea del requerimiento con carácter general o en determinados supuestos

El primer modo de intervención se articula mediante la notificación simultánea del requerimiento al proveedor de servicios que se encuentre en su territorio y a la autoridad del Estado parte designada a tal efecto[88]. Se trata de una facultad de control *ex ante* que, en cierta medida, recuerda a la

88. El Estado parte deberá, necesariamente, indicar una autoridad concreta —y única— a la que habrá de remitirse tal información; para facilitar que el resto de los Estados parte tengan conocimiento de estas —y de su información de contacto—, la Secretaría Ge-

obligación de notificar a la autoridad de ejecución prevista por el Reglamento de Prueba Electrónica de la Unión Europea cuando se solicita la entrega de datos de tráfico o de contenido[89]. El art. 7.5.a) del Segundo Protocolo introduce esta posibilidad para los datos de los abonados y la regula de manera amplia en todos sus extremos; no obstante, como hemos anticipado, se caracteriza por su voluntariedad, de modo que corresponde a cada Estado parte decidir si quiere exigirla o no. Como apunta MARCÉN, esto puede traer como consecuencia la fragmentación del régimen establecido por el Protocolo[90], pero, en todo caso, se considera aconsejable que los Estados parte requieran esta notificación a efectos de conceder mayor seguridad jurídica a todos los sujetos implicados[91].

Primero, esta notificación simultánea puede exigirse con carácter general para todos los requerimientos que tengan como receptor a un proveedor de servicios que se encuentre en su territorio, o puede limitarse a determinados supuestos si concurren una serie de circunstancias preestablecidas. Segundo, esto puede exigirse en cualquier momento por el Estado parte —no solo cuando firme el Protocolo o realice el depósito de su instrumento de ratificación, aceptación o aprobación, sino también posteriormente—, y es suficiente para ello con notificar la inclusión de este requisito a la Secretaría General del Consejo de Europa —por tanto, no ha de formular una declaración al respecto—; del mismo modo, nada debe impedir al Estado parte que optó por establecer la notificación con carácter obligatorio, eliminarla o modifi-

---

neral del Consejo de Europa se encargará de crear y mantener actualizado un registro [art. 7.5.e) y f)].

89. Para un análisis detallado de la notificación simultánea de la orden europea de producción a la autoridad de ejecución como mecanismo para permitir su control *ex ante*, *vid*., DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…*, *op. cit*., pp. 53 a 56; LLOPIS NADAL, P. "La cooperación judicial penal con el entorno digital como escenario…", *op. cit*., pp. 464 a 468.

90. GASCÓN MARCÉN, A., "The push for the international regulation of cross-border Access to electronic evidence…", p. 401.

91. *Ibidem*, p. 397. La autora fundamenta la oportunidad de exigir esta notificación en los comentarios presentados por *European Internet Service Provider Association* (*EuroISPA*) al texto provisional del Segundo Protocolo; con base en la importancia de esta salvaguardia, la asociación mantuvo entre sus recomendaciones que la autoridad designada por el Estado parte donde se encuentre el particular requerido debería ser notificada en todas las circunstancias, tanto por seguridad jurídica como para evitar cargas adicionales al proveedor de servicios [EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, p. 3 (disponible en: https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab, última consulta: 25 de abril de 2025).

car su régimen en cualquier momento posterior[92]. Y, tercero, la notificación que se remitirá simultáneamente a la autoridad del Estado parte requerido habrá de ser detallada, integrando no solo el requerimiento que recibe el proveedor, sino también, necesariamente, la información complementaria que exige el art. 7.4 y un resumen de los hechos de la causa penal para la que se solicitan los datos.

5.2. La posibilidad de que el Estado parte exija la consulta previa del proveedor de servicios en determinados supuestos

El segundo modo de intervención del Estado parte requerido —que puede coexistir o no con el primero—, consiste en prever en su ordenamiento jurídico interno una disposición obligando a los proveedores de servicios que se encuentren en su territorio a consultar a las autoridades estatales, cuando reciban un requerimiento con base en este procedimiento de cooperación directa, con carácter previo a revelar la información. Del mismo modo que sucede con la notificación, esta consulta obligatoria podrá introducirse, eliminarse o modificarse en cualquier momento por el legislador nacional. Sin embargo, al contrario del primer tipo de intervención, el art. 7.5.b) solo permite que la consulta se llevé a cabo en circunstancias determinadas —y no con carácter general—, una restricción que se impone motivada por el propósito de agilizar la obtención de los datos en posesión de particulares ubicados en otra jurisdicción —fin último de esta medida— y eliminar fases o etapas intermedias en el intercambio entre la autoridad emisora y el proveedor de servicios[93].

El Informe explicativo proporciona algunas ideas sobre en qué situaciones esta consulta previa podría exigirse, entre otras, cuando fuera posible aplicar un motivo de denegación o pudiera verse afectado el proceso penal que se desarrolla en el Estado parte requerido[94]. En cualquier caso, no parece sencillo articular las causas que justifican una consulta previa con el conocimiento de estas por parte del proveedor de servicios, en especial, si, como particular —ente de naturaleza privada—, no solo desconoce los procesos penales que están en curso ante los tribunales del Estado en cuyo territorio se encuentra, sino que, además, recibe un requerimiento en el que no consta parte de la información sobre el proceso penal que se está desa-

92. En este sentido, Informe explicativo al Segundo Protocolo adicional, apartado 114.
93. Exigir consultas para todos los requerimientos con carácter general "añadiría un paso adicional que podría retrasar significativamente la tramitación de las solicitudes" (Informe explicativo al Segundo Protocolo adicional, apartado 108).
94. Informe explicativo al Segundo Protocolo adicional, apartado 108, *in fine*.

rrollando en el Estado parte que requiere los datos —por ejemplo, no tendrá conocimiento de los hechos, solo del delito o delitos que han motivado la causa—. Todo lo indicado podría tener como consecuencia que las consultas a la autoridad del Estado parten donde se encuentra el propio proveedor de servicios terminaran siendo más frecuentes de lo deseado para la rapidez que cabe esperar de esta medida de cooperación directa.

5.3. Las distintas actuaciones de la autoridad del Estado parte notificada simultáneamente o consultada por el proveedor de servicios

La autoridad designada por el Estado parte en cuyo territorio se encuentra el proveedor de servicios requerido, tras recibir la notificación remitida por la autoridad competente, o la consulta del particular en posesión de los datos, deberá adoptar una decisión al respecto. Ahora bien, de antemano, se prevé la posibilidad de que solicite información adicional para valorar si accede o deniega la entrega[95]; esta se pedirá a la autoridad del Estado parte emisor a la que deben enviarse los datos relativos a los abonados —pues nos remite al art. 7.4.c)—, algo que, de nuevo, plantea la duda de si se trata de la autoridad emisora, de la autoridad que necesita la información —cuando ambas no coincidan—, o de una tercera autoridad responsable de centralizar todo lo relativo a los requerimientos emitidos sobre la base de esta medida de cooperación directa.

Además, aunque el Segundo Protocolo no dice nada al respecto, el Informe explicativo enuncia la posibilidad de que el legislador nacional del Estado parte que opte por intervenir de algún modo en esta cooperación directa —exigiendo la notificación simultánea o la consulta previa—, imponga a los proveedores de servicios un plazo de espera. Este plazo podría incluirse entre las medidas adoptadas por el Estado parte para cumplir con la obligación asumida en virtud del art. 7.2.a) —es decir, para permitir a los proveedores de su territorio entregar los datos— y su propósito sería garantizar que, efectivamente, se practica la notificación o se realiza la consulta[96].

95. No se detalla en qué puede consistir tal información adicional que puede solicitarse, de modo que podría ir desde dotar de mayor precisión a la información remitida —en especial, a los hechos de la causa, al delito o los delitos objeto del proceso y a las disposiciones nacionales aplicables—, en justificar que, efectivamente, se respeta la proporcionalidad en la solicitud de los datos —la relación entre gravedad del delito y la afectación de los derechos fundamentales— o en explicar el motivo por el cual se sujeta la entrega a instrucciones procesales especiales —por ejemplo, la exigencia de confidencialidad—.

96. Informe explicativo al Segundo Protocolo adicional, apartado 112.

Tras hacer uso —o no— de esta posibilidad de pedir información adicional, la autoridad que ha sido notificada o consultada habrá de dar una respuesta. Esta puede consistir en aceptar la entrega de los datos solicitados o en denegarla. En este último caso, cuando ordene al proveedor de servicios que se encuentra en su territorio que no revele la información relativa a los abonados, deberá justificar su decisión y, además, deberá hacerlo sobre la base de los motivos —entendemos, tasados— que prevé el propio art. 7.5.c) —de modo que, al adoptar las medidas nacionales necesarias en relación con la notificación o consulta en el marco de este procedimiento de cooperación directa, el legislador del Estado parte no podrá ampliar las situaciones que permiten denegar la entrega de los datos, puesto que la regla general ha de ser la cooperación directa por parte del proveedor de servicios—[97].

Así, como primer motivo, la negativa puede justificarse por el hecho de que en el Estado parte requerido hay en estos momentos —o habrá en un futuro inmediato— procesos penales en curso —en fase de investigación o en fase de enjuiciamiento— que pueden verse perjudicados por la revelación de los datos solicitados. Como segundo motivo para denegar la cooperación directa se permite hacer uso de las causas reguladas en el Convenio para los supuestos en que se solicitan las pruebas electrónicas a través de la asistencia mutua —algo que se realiza mediante una remisión expresa a los arts. 25.4 y 27.4 de la norma adoptada en 2001—. De ese modo, la entrega de los datos puede condicionarse a lo que prevea el derecho interno del Estado parte en cuyo territorio se encuentra el proveedor de servicios y a lo establecido en los tratados sobre asistencia mutua que pudieran ser aplicables —e, incluso, se permite aplicar los motivos por los que el Estado puede denegar la cooperación—. Asimismo, esta negativa puede fundamentarse en el hecho de que la información se requiere para un proceso penal por un delito político —o vinculado a un delito de estas características— y cuando se considere que la entrega de los datos solicitados puede atentar contra intereses esenciales del Estado —por ejemplo, su soberanía, seguridad u orden público—[98].

En el caso de que la autoridad que ha sido notificada o consultada decida denegar la entrega de los datos relativos a los abonados, deberá, en primer lugar, ordenar al proveedor de servicios que se encuentra en su territorio que no revele la información. Adicionalmente, pondrá su decisión en cono-

97. La misma interpretación podemos extraer del Informe explicativo, donde se mantiene la idea de que "la cooperación debe ser, en principio, amplia, y los impedimentos deben estar estrictamente limitados" (Informe explicativo al Segundo Protocolo adicional, apartado 110).

98. BUJOSA VADELL, L., "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", *op. cit.*, p. 76.

cimiento de la autoridad del Estado parte a la que esta información debía ser enviada —de nuevo, la disposición nos remite a la autoridad del art. 7.4.c)—, esto habrá de realizarse, en todo caso, de manera motivada —es decir, justificando la negativa conforme a lo expuesto en el párrafo precedente— y actuando sin demoras indebidas —a efectos de respetar la celeridad que se espera de esta nueva medida de cooperación directa—.

6. LA NEGATIVA O INACTIVIDAD DEL PROVEEDOR DE SERVICIOS Y EL RECURSO A LA COOPERACIÓN INTERNACIONAL O A LA ASISTENCIA MUTUA COMO ALTERNATIVA

6.1. Las posibles conductas del proveedor de servicios requerido y la posibilidad de exigir que motive toda negativa e inactividad

El proveedor de servicios al que la autoridad competente de otro Estado parte solicita la información relativa a los abonados puede responder ante esta petición de tres maneras distintas. En primer lugar, puede entregar los datos, cumpliendo con el plazo establecido por la autoridad competente en su requerimiento —o, en su defecto, en un plazo inferior a treinta días, tal y como se desprende del art. 7.7—. En segundo lugar, puede comunicar expresamente su negativa a entregar los datos a la autoridad que emitió el requerimiento. Y, en tercer lugar, puede mantenerse inactivo, esto es, no proporcionar ningún tipo de respuesta dentro de los treinta días siguientes a la recepción de la solicitud o, en el caso de que sea superior, en el plazo indicado en el requerimiento por la autoridad emisora[99].

El proveedor de servicios puede negarse a entregar la información o mantenerse inactivo incluso cuando la autoridad designada por el Estado parte en cuyo territorio se encuentra —conforme a lo expuesto *supra*—, haya sido notificada o consultada con carácter previo y no haya manifestado oposición alguna a que la información sea revelada. Asimismo, como particular, el proveedor de servicios podrá negarse o mantenerse inactivo, no solo cuando, según el derecho interno del Estado parte en cuyo territorio se encuentra, la entrega de los datos sea facultativa, sino, también, cuando tenga carácter obligatorio a condición de que se cumplan los requisitos formales —cuestión distinta es si, posteriormente, será sancionado por ello—.

99. En cualquier caso, se espera que en el plazo previsto el proveedor de servicios realice todas las actividades oportunas en relación con el requerimiento recibido, incluida la notificación o consulta a la autoridad de su Estado, si procede (Informe explicativo al Segundo Protocolo adicional, apartado 119).

Finalmente, en caso de negativa a entregar los datos —y, entendemos, también cuando se mantenga inactivo—, se puede exigir al proveedor que motive su decisión de no revelar la información requerida. El art. 7.7 del Segundo Protocolo dice, expresamente, que son "las Partes" quienes podrán pedir tal justificación; por tanto, prevalece la duda de qué parte puede solicitarlo, si el Estado parte que emitió el requerimiento o el Estado parte en cuyo territorio se encuentra el proveedor. Es cierto que, si la exigencia de motivar se prevé en la legislación nacional por la que se adoptan las medidas para permitir a los proveedores entregar la información, esta sería vinculante para quien se negara —o mantuviera inactivo—, pues queda sujeto a las disposiciones de este ordenamiento. Sin embargo, a quien interesa realmente conocer los motivos de esta negativa —o inactividad— es al Estado parte cuya autoridad ha emitido el requerimiento, pues con base en estos, podrá decidir si intenta o no obtener la información a través de la cooperación internacional entre autoridades estatales[100]; en tal caso, la petición de motivar se incluiría expresamente en el requerimiento que se hace llegar al proveedor de servicios, pero no tendría carácter vinculante para este.

6.2. Las alternativas de la autoridad competente para obtener la información ante la negativa o inactividad del proveedor de servicios

El proveedor de servicios, ente de naturaleza privada sujeto al ordenamiento jurídico de un Estado distinto al que le requiere la información, puede negarse a entregar los datos relativos a los abonados o mantenerse inactivo frente al requerimiento recibido; ante cualquiera de estas dos situaciones, el Segundo Protocolo no prevé un procedimiento de ejecución *ad hoc*, sino que remite a las distintas formas de cooperación entre autoridades estatales. Así, el art. 7.7 establece que se podrá "intentar ejecutar el requerimiento *únicamente* en virtud del artículo 8 o por medio de otras formas de asistencia mutua" (cursivas de la autora); en consecuencia, incluso cuando la autoridad emisora considere que el incumplimiento no está justificado, no podrá recurrir a la autoridad del Estado parte en cuyo territorio se encuentra el proveedor de servicios para solicitarle que examine el requerimiento y, si procede, que adopte las medidas necesarias para la ejecución, obligando al proveedor que se encuentra bajo su jurisdicción a entregar los datos —un procedimiento que sí prevé el Reglamento de Prueba Electrónica de la Unión Europea y que sería útil para agilizar el intercambio[101]—.

100. Así, por ejemplo, si el proveedor de servicios justifica su negativa en que, por cualquier motivo, ya no dispone de los datos, no tendrá sentido recurrir a otras vías para obtener la información (Informe explicativo al Segundo Protocolo adicional, apartado 119, *in fine*).

101. Para un análisis detallado de la intervención de la autoridad de ejecución cuando el prestador de servicios no cumple con la orden europea de producción o de conserva-

Por tanto, la autoridad emisora del requerimiento solo podrá hacer uso de la asistencia mutua para solicitar los datos que el proveedor de servicios no le ha facilitado, pudiendo valerse, a tal fin, de cualquier instrumento existente —entre otros, de los regulados en el Convenio y de los introducidos por el Segundo Protocolo—. Con mención expresa en el art. 7.7, debemos destacar el procedimiento de cooperación internacional introducido en virtud del art. 8 del Segundo Protocolo con el propósito de "dar efecto" —entendido como validar, aceptar, refrendar[102]— a los requerimientos de otro Estado parte solicitando la entrega rápida de información relativa a los abonados o de datos relativos al tráfico; para ello, cuando se emita la solicitud dirigida a la autoridad de otro Estado parte con base en el art. 8, entre la información complementaria podrá incluirse una referencia a que los datos ya han sido solicitados por otros medios [(art. 8..3.b).viii)][103]. En cualquier caso, la falta de un auténtico procedimiento de ejecución y la solución de remitir a los instrumentos de asistencia mutua puede provocar, aun cuando estos sean novedosos y se imponga la celeridad, que la autoridad que precisa de las pruebas electrónicas no disponga de ellas en el momento adecuado para un buen fin del proceso penal en curso.

VI. CONCLUSIÓN

La posibilidad de articular la cooperación directa con entes del sector privado en el marco de un proceso penal constituye un relevante avance; ello es así gracias a la celeridad que se logra al prescindir de autoridades que actúen como intermediarias en la obtención transfronteriza de los datos que permitirán identificar a la persona o ponerse en contacto con ella. Ahora bien, aunque es cierto que los arts. 6 y 7 del Segundo Protocolo, una vez introducidos por los legisladores nacionales en sus correspondientes ordenamientos, facilitarán la tarea de las autoridades encargadas de la investigación penal y

ción, *vid*., DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…, op. cit*., pp. 76 a 80; LLOPIS NADAL, P. "La cooperación judicial penal con el entorno digital como escenario…", *op. cit*., pp. 471 y 472.

102. Informe explicativo al Segundo Protocolo adicional, apartado 129.

103. El Informe explicativo enuncia que para obtener la ejecución del requerimiento a partir del mecanismo de cooperación internacional regulado en el art. 8 "el presente Protocolo contempla un procedimiento simplificado para la conversión de una orden emitida en virtud de este artículo [refiriéndose al art. 7] en una orden en virtud del artículo 8 a fin de aumentar las posibilidades de la Parte emisora para obtener información relativa al abonado" (Informe explicativo al Segundo Protocolo adicional, apartado 118). No obstante, más allá de la previsión indicada en cuanto al contenido del requerimiento no encontramos otra mención en el art. 8.

reducirán los tiempos para disponer de la información, no es menos cierto que esta cooperación directa podría traer aparejadas otras consecuencias. En este sentido, no debemos perder de vista dos cosas.

Por una parte, que tras estas medidas hay derechos fundamentales que podrían verse afectados —la protección de datos o la intimidad—, y que el uso efectivo de la información obtenida en un proceso penal ha de hacerse con pleno respeto de los derechos de la defensa —asegurando la integridad de los datos e informando a su titular sin demora, siempre que el respeto de la confidencialidad lo permita—. Por otra parte, que en este novedoso modelo, quien decide es un particular —normalmente una empresa que desarrolla sus actividades con fines económicos—, que actuará conforme a sus propias motivaciones —las cuales, según las circunstancias, pueden ir desde el temor a la pérdida de clientes o a que estos le exijan responsabilidades, hasta sentirse coaccionado por una normativa que le obliga a entregar la información, debiendo justificar toda negativa—; además, esto lo hará, como regla general, sin contar con una autoridad estatal que supervise lo solicitado por la autoridad de otro Estado parte y sujeto a unos plazos de actuación que se espera que sean reducidos y, por ello, que pueden ir en detrimento de las garantías exigibles.

A lo indicado debemos añadir que el refuerzo de la cooperación directa que se articula entre las autoridades de un Estado parte y los prestadores de servicios que se encuentran en el territorio de otro Estado parte ha sido tímido. Esto debe mantenerse, en especial, si lo comparamos con la cooperación directa que regula el Derecho de la Unión Europea en su reciente Reglamento de Prueba Electrónica, con lo que se estableció hace dos décadas mediante el art. 18 del Convenio para el ámbito interno o con lo que se venía realizando en la práctica de manera voluntaria por los propios prestadores de servicios.

Así, si bien el art. 18 del Convenio permite solicitar a las personas que se encuentran en el Estado parte de la autoridad que requiere la información la entrega de datos informáticos que posean o que estén bajo su control, no se hace referencia alguna a esto al tratar la cooperación directa en el articulado del Segundo Protocolo —restringiéndola a las entidades que prestan servicios en la sociedad de la información—. Además, la posibilidad de solicitar información de manera directa a los prestadores de servicios con base en los arts. 6 y 7 se limita a los datos menos invasivos —los que permiten identificar a una persona o contactar con ella—; en cambio, los datos más sensibles —esto es, los de tráfico y los de contenido— solo pueden obtenerse mediante la cooperación entre autoridades. Por último, también

es reseñable el hecho de que no se prevea un procedimiento de ejecución propio, por parte de la autoridad del Estado parte donde se encuentra el particular requerido, para el caso de que este no responda con la entrega de los datos en el plazo previsto para ello.

En cualquier caso, debemos destacar el otro refuerzo de la cooperación para la obtención de pruebas electrónicas introducido por el Segundo Protocolo: la cooperación rápida y en casos de emergencia que se regula con detalle en los arts. 8 a 10. Bajo las secciones tituladas "procedimientos que refuerzan la cooperación internacional entre autoridades a efectos de la revelación de datos informáticos almacenados" (arts. 8 y 9) y "procedimientos de asistencia mutua en situaciones de emergencia" (art. 10), estas medidas, si bien no permiten una cooperación directa con el particular que está en posesión de los datos —y, por ello, no podrán reducir tanto los plazos de entrega—, son, si cabe, más relevantes y tendrán, previsiblemente, mayor incidencia que las reguladas en los arts. 6 y 7. Ello es así porque se podrán utilizar cuando el ente de naturaleza privada requerido, por el motivo que sea, no haya accedido a entregar la información a la autoridad de otro Estado parte y, además, porque con estas medidas no solo será posible solicitar datos de los abonados, sino que también se podrá requerir la entrega de datos de tráfico y datos de contenido en posesión de los prestadores de servicios que se encuentran en el territorio de otro Estado parte[104].

BIBLIOGRAFÍA Y OTRAS FUENTES CONSULTADAS

1. BIBLIOGRAFÍA

ASENCIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", en FERNÁNDEZ LÓPEZ, M. y ASENCIO MELLADO, J. M, *Justicia penal y nuevas formas de delincuencia,* Tirant lo Blanch, 2017, pp. 44-67.

BAHAMONDE BLANCO, M., "Segundo Protocolo Adicional al Convenio de Budapest: Nuevos medios para la cooperación penal y la obtención de prueba electrónica", *La Ley Penal*, núm. 157 (2022), pp. 1-17.

104. Para una exposición más detallada de estas medidas de cooperación internacional y de asistencia mutua, *vid*., DE HOYOS SANCHO, M., "Novedades en materia de obtención transfronteriza de información electrónica…", *op. cit.*, pp. 121 a 123; DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica…*, *op. cit.*, pp. 130 a 132; GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., "El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad", *op. cit.*, pp. 29 a 34.

BUJOSA VADELL, L., "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", en FONTESTAD PORTALÉS, L. y JIMÉNEZ LÓPEZ, M. N., *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, Thomson Reuters-Aranzadi, 2022, pp. 69-97.

CERRATO GURI, E., "Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de prueba electrónica", *Revista General de Derecho Europeo*, núm. 61 (2023), pp. 156-187.

DELGADO MARTÍN, J., "Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", *Diario La Ley*, núm. 10358 (2023), pp. 1-8.

DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre la obtención transfronteriza de información electrónica en procesos penales: Análisis y valoración del "e-evidence package"*, Aranzadi-La Ley, Madrid, 2024.

DE HOYOS SANCHO, M., "Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo", *Revista de Estudios Europeos*, núm. extraordinario monográfico (2023), pp. 99-128.

GARCÍA SÁNCHEZ, M. D., *Medidas cautelares cibernéticas: una nueva oportunidad en la lucha contra la ciberdelincuencia*, Atelier, Barcelona, 2024.

GASCÓN MARCÉN, A., "The Budapest Convention and the UN Cybercrime Convention negotiations", en SEGURA SERRANO, A., *Global cybersecurity and International Law,* Routledge, 2024, pp. 174-192.

GASCÓN MARCÉN, A., "The push for the international regulation of cross-border Access to electronic evidence and human rights", *Cuadernos de Derecho Transnacional*, vol. 15, núm. 1 (2023), pp. 385-402.

GASCÓN MARCÉN, A., "Improving access to electronic evidence: the European normative struggle", en *Cybercrime: new threats, new responses: Actas del XV.º Congreso Internacional Internet, Derecho y Política,* Universitat Oberta de Catalunya, 2020, pp. 140-157.

GASCÓN MARCÉN, A., "La mejora de la obtención de pruebas electrónicas: avance necesario para la seguridad europea", en *La Unión Europea y la seguridad: defensa de los espacios e intereses comunes,* ICEI Ocassional Papers, 2018, pp. 16-21.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., "El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad", *Revista General de Derecho Procesal*, núm. 58 (2022), pp. 1-46.

JARIEGO RUIZ, M.ª, "Ciberdelincuencia: amenaza en la red y la oportunidad del Convenio de Budapest", *Diario La Ley*, núm. 10358 (2023), pp. 1-26.

LLOPIS NADAL, P., "La cooperación judicial penal con el entorno digital como escenario: los prestadores de servicios como coprotagonistas del Reglamento 2023/1543 sobre las órdenes europeas de producción y de conservación a efectos de prueba electrónica", en CASTELLÓ PASTOR, J. J., *Análisis del Reglamento (UE) de Servicios Digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 433-476.

SIGNORATO, S., "Cross-border gathering of e-evidence: different legal frameworks in European Union and Council of Europe", *Journal of Eastern European Criminal Law*, núm. 1 (2023), pp. 9-18.

TEJADA DE LA FUENTE, E., Entrevista — Ciberderecho, *Diario La Ley*, 24 de mayo de 2022, pp. 1-6.

VELASCO NÚÑEZ, E., "El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", *Diario La Ley*, núm. 62 (2022), pp. 1-7.

2. OTRAS FUENTES CONSULTADAS

EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime (disponible en: https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab, última consulta: 25 de abril de 2025).

Informe explicativo al Convenio sobre la Ciberdelincuencia (disponible en: https://rm.coe.int/16802fa403, última consulta, 20 de abril de 2025).

Informe explicativo al Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas, Serie de Tratados del Consejo de Europa, n.º 224, de 12 de mayo de 2022 (disponible en: https://rm.coe.int/1680a83723, última consulta, 17 de abril de 2025).

SIRIUS Project, Cross-border Access to electronic Evidence, "Article 6 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Direct Requests for Domain Name Registration Information", last update: 23/01/2024, Eurojust — Europol (disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/requests-for-domain-name-registration-information-under-article-6-of-the-second-additional-pro-

tocol-to-the-convention-on-cybercrime-23-01-2024.pdf, última consulta: 18 de abril de 2025).

SIRIUS Project, Cross-border Access to electronic Evidence, "Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscribers information", last update: 23/01/2024, Eurojust — Europol, pág. 5 (disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/production-orders-for-the-disclosure-of-subscriber-information-under-article-7-of-the-second-additional-protocol-to-the-convention-on-cybercrime-23-01-2024.pdf, última consulta: 18 de abril de 2025).

T-CY (Cybercrime Convention Committee), Guidance note #10 Production orders for subscriber information (Article 18 Budapest Convention), T-CY(2015)16, 28 February 2017 (disponible en: https://rm.coe.int/16806f943e, última consulta: 25 de abril de 2025).

Papel + Digital

ESTUDIOS

Acceso online a Biblioteca Digital Legalteca:
consulte página inicial de esta obra

La presente obra colectiva surge de la necesidad de reflexionar sobre las múltiples dimensiones que adopta el Derecho en el contexto digital, abarcando desde la protección de los consumidores hasta el impacto de la inteligencia artificial en la gobernanza global. A lo largo de sus doce capítulos, la obra aborda cuestiones de plena actualidad, como la vulnerabilidad del consumidor en línea, la protección de menores en entornos digitales, la regulación de los patrones oscuros, los mecanismos alternativos de resolución de litigios y la obtención de pruebas electrónicas. También se analizan los complejos desafíos que plantean la sucesión de bienes digitales y la consideración de los datos como bienes transnacionales. Destaca, además, el desarrollo normativo impulsado desde la Unión Europea y su diálogo con el Derecho internacional, orientado a adaptar los marcos regulatorios a los retos de la digitalización. En especial, se examina el papel de la inteligencia artificial en sus múltiples dimensiones: responsabilidad, derechos digitales, desinformación y riesgos sistémicos.

En su conjunto, se ofrece una visión de los esfuerzos legislativos —principalmente desde la Unión Europea— orientados a promover una transición digital centrada en la persona que preserve las garantías y los valores democráticos. Estos estudios representan una aportación significativa al debate sobre la evolución del Derecho en el entorno digital.

Esta obra colectiva es fruto de las reflexiones alcanzadas en la segunda etapa del proyecto de investigación del Ministerio de Ciencia, Innovación y Universidades titulado «Hacia una transición digital centrada en la persona en la Unión Europea» TED 2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea «NextGenerationEU»/PRTR cuyos autores forman parte del equipo de investigación y de trabajo.

ISBN: 978-84-1163-776-3

AENOR GESTIÓN DE LA CALIDAD ISO 9001 ER-0280/2005 · IQNET RECOGNIZED CERTIFICATION · AENOR GESTIÓN AMBIENTAL ISO 14001 GA-2005/0100

Proyecto TED 2021-129307A-I00 financiado por:

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · Financiado por la Unión Europea NextGenerationEU · Plan de Recuperación, Transformación y Resiliencia · AGENCIA ESTATAL DE INVESTIGACIÓN

ARANZADI