# EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS COMO MODELO DE LAS RECIENTES PROPUESTAS DE LEGISLACIÓN DIGITAL EUROPEA

# THE GENERAL DATA PROTECTION REGULATION AS A MODEL OF RECENT EUROPEAN DIGITAL DRAFT LEGISLATION

Ana Gascón Marcén
*Profesora Contratada Doctora de Derecho Internacional Público*
*Universidad de Zaragoza*

Recibido: 11.06.2021 / Aceptado: 06.07.2021
DOI: https://doi.org/10.20318/cdt.2021.6256

**Resumen:** Este artículo explica el impacto del Reglamento General de Protección de Datos en las subsiguientes propuestas de la Comisión Europea en el marco del mercado único digital. Se estudia en particular su influencia en el Reglamento e-privacy, el Reglamento de las órdenes europeas de entrega y conservación de pruebas electrónicas, el Reglamento para la prevención de la difusión de contenidos terroristas en línea, la Ley de Servicios Digitales, la Ley de Mercados Digitales y la Ley de Inteligencia Artificial. Concretamente, se presta atención a los mecanismos que buscan mejorar la aplicación de estas normas a intermediarios situados fuera de la Unión Europea como son su aplicación extraterritorial o la obligación de que nombren a un representante en la misma.

**Palabras clave:** Reglamento General de Protección de Datos, Reglamento e-privacy, la Ley de Servicios Digitales, Ley de Mercados Digitales, Ley de Inteligencia Artificial.

**Abstract:** This paper explains the impact of the General Data Protection Regulation on the subsequent proposals of the European Commission in the framework of the digital single market. It studies its influence on the e-privacy Regulation, the Regulation on European production and preservation orders for electronic evidence, the Regulation on preventing the dissemination of terrorist content online, the Digital Services Act, the Digital Markets Act and the Artificial Intelligence Act. Specifically, attention is paid to the mechanisms that seek to improve the application of these rules to intermediaries located outside the European Union, such as their extraterritorial application or the obligation to appoint a representative within it.

**Keywords:** General Data Protection Regulation, e-privacy Regulation, Digital Services Act, Digital Markets Act, Artificial Intelligence Act.

## I. Introducción

**1**. El Reglamento General de Protección de Datos (RGPD)[1] se ha convertido desde que empezó a aplicarse en 2018[2] en una de las normas más conocidas de la Unión Europea (UE)[3] y con una mayor influencia fuera de sus fronteras. Por una parte, son múltiples lo países que han hecho converger con él sus legislaciones nacionales, entre otras razones, para conseguir una decisión de adecuación que facilite el flujo de datos personales entre los mismos y el Espacio Económico Europeo[4], como ha ocurrido con Estados tan lejanos como Corea del Sur o Japón.[5] A esto se suma que la mayoría de nuevas propuestas de normas de protección de datos de casi todos los países del mundo permiten ver una influencia más o menos fuerte del mismo.[6] Es incluso el caso de China.[7] El RGPD se ha convertido en una especie de estándar de oro (*gold standard*) en el ámbito de la protección de datos personales.[8] Las normas del RGPD son consideradas como la tercera generación de reglas de protección de datos personales[9] y se usan como parámetro de medida para valorar cómo de modernas son las leyes que se van adoptando en todo el mundo.[10]

**2.** A esto se suma que muchas empresas fuera de Europa están adaptando sus operaciones para cumplir con el RGPD, incluso cuando no están obligadas legalmente. Esto reviste normalmente dos formas: vertical (donde las empresas multinacionales con algunas operaciones en la UE quieren coherencia

[1] 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), *DOUE* L 119, de 4 de mayo de 2016, p. 1.

[2] Si bien el RGPD entró en vigor el 24 de mayo de 2016, empezó a aplicarse a partir del 25 de mayo de 2018 (art. 99 RGPD). Estos dos años de plazo tenían como objetivo permitir la adecuación de las empresas y las administraciones públicas al mismo.

[3] En un Eurobarómetro especial realizado un año después de que empezará a aplicarse el RGPD, el 67% de los encuestados había oído hablar del RGPD, y, además, un 73% de los mismos habían oído hablar de al menos un derecho garantizado por el RGPD. Véase Kantar, *Special Eurobarometer 487a The General Data Protection Regulation*, European Commission, 2019, p. 2.

[4] Para conseguir una decisión de adecuación, la Comisión Europea hace un análisis pormenorizado de: la legislación, la jurisprudencia, el reconocimiento a los interesados de derechos exigibles y de recursos administrativos y acciones judiciales que sean efectivos, la existencia de una autoridad de control independientes con poderes de ejecución adecuados y los compromisos internacionales asumidos por el país (art. 45 RGPD). Para que se dé la decisión de adecuación, la Comisión debe concluir de este análisis que el Estado ofrece un nivel de protección esencialmente equivalente al de la UE. Véase J. J. Gonzalo Domenech, "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros", *Cuadernos de Derecho Transnacional*, vol. 11, nº 1, 2019, pp. 350-371, DOI: https://doi.org/10.20318/cdt.2019.4624 (todas las páginas web consultadas para este trabajo lo han sido por última vez el 11 de junio de 2021) y C. I. Cordero Álvarez, "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act", *Revista Española de Derecho Europeo*, nº. 70, 2019, pp. 49-107.

[5] Véase A. Gascón Marcén, "The New Personal Data Protection in Japan: Is It Enough?", en *Media technologies for work and play in East Asia: Critical perspectives on Japan and the two Koreas*, Bristol University Press, 2021, pp. 101-120 y de la misma autora, "Japón y la Unión Europea: la mayor área mundial de flujos de datos personales seguros", en *Derecho, Empresa y Administración Pública en Japón,* Tirant Lo Blanch, 2021, pp. 59-82.

[6] Véase G. Greenleaf y B. Cottier, "2020 Ends a Decade of 62 New Data Privacy Laws", *Privacy Laws & Business International Report*, nº 163, 2020, pp. 24-26.

[7] G. Zhang y K. Yin, "A look at China's draft of Personal Information Protection Law", *IAPP,* 26/10/2020. Disponible en: https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/

[8] Véase G. Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016)." *International Data Privacy Law*, nº 6, 2016, pp. 77-78; y A. Mantelero, "The future of data protection: Gold standard vs. global standard", *Computer Law & Security Review*, vol. 40, 2020. https://doi.org/10.1016/j.clsr.2020.105500

[9] Las normas de primera generación estarían recogidas en las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE de 1980 y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa de 1981 (conocido como Convenio 108). Las normas de segunda generación estarían recogidas en la 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. Véase G. Greenleaf, "International data privacy agreements after the GDPR and Schrems", *Privacy Laws & Business International Report*, nº 139, 2016, pp. 12-15, y del mismo autor "European' data privacy standards implemented in laws outside Europe", *Privacy Laws & Business International Report, vol*. 149, 2017, pp. 21-23

[10] Véase, como ejemplo, G. Greenleaf, "Jamaica Adopts a Post-GDPR Data Privacy Law" *Privacy Laws & Business International Report*, nº 167, 2020, pp. 5-8, http://dx.doi.org/10.2139/ssrn.3712745 y G. Greenleaf y B. Cottier, "Data Privacy Laws and Bills: Growth in Africa, GDPR Influence", *Privacy Laws & Business International Report*, nº 152, 2018, pp. 11-13.

global) y horizontal (en acuerdos de empresa a empresa (B2B) en los que las empresas quieren que sus proveedores cumplan con el RGPD).[11] Un ejemplo de esto sería Microsoft.[12] Este fenómeno se ha bautizado como el "efecto Bruselas"[13] que consiste en que los estándares europeos terminan aplicándose en todo el mundo, porque las empresas quieren acceder al mercado único y terminan así aplicando y exportando sus normas a nivel global, siendo uno de los casos comúnmente usados como ejemplo el de la protección de datos personales.

**3.** Según Schwartz, dos factores primordiales han promovido la difusión mundial de la normativa europea de protección de datos. El primero se refiere al fondo legal. El discurso público sobre la privacidad del consumidor ha evolucionado drásticamente, e instituciones importantes y personas prominentes en muchas jurisdicciones no pertenecientes a la UE reconocen ahora el atractivo de la protección de datos al estilo de la UE. Más allá del fondo, la UE se ha beneficiado de la accesibilidad de su enfoque legislativo general; otras jurisdicciones se han visto atraídas por el modelo legal altamente trasplantable de la UE. Según este autor, la UE está siendo recompensada por su éxito en el mercado de las ideas reguladoras.[14]

**4.** No obstante, el RGPD también ha sido ampliamente criticado por crear una elevada carga burocrática a las empresas, ser excesivamente formalista y limitar la innovación.[15] Los Estados Unidos consideran que su aplicación supone una barrera desproporcionada al comercio que afecta a todos los Estados fuera de la UE.[16] El Vicepresidente de Google ha animado a Estados Unidos a aceptar la invitación de la UE de crear un Consejo de Comercio y Tecnología UE-EEUU,[17] porque en su opinión la UE está adoptando unilateralmente nuevas regulaciones digitales dirigidas directamente a empresas con sede en el extranjero.[18]

---

[11] Véase G. Greenleaf, *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi,* 25 May 2018. UNSW Law Research Paper No. 18-56, p. 4 Disponible en: http://dx.doi.org/10.2139/ssrn.3184548 Es lo que el autor define como "GDPR creep" y que considera que puede ser tan importante como la convergencia legislativa.

[12] Véase J. Brill, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft Blog,* 21/5/2018. Disponible en: https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

[13] Véase A. Bradford, *The Brussels Effect. How the European Union rules the world.* Oxford University Press, 2020. Si bien ha empezado a teorizarse también la existencia de un "efecto Beijing". Véase M. S. Erie y T. Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", *New York University Journal of International Law and Politics*, 2021. Disponible en: https://ssrn.com/abstract=3810256 En este artículo, los autores defienden que China da forma a la gobernanza de datos transnacional al proporcionar infraestructura digital a los mercados emergentes y por ser un ejemplo de "soberanía de los datos" y desarrollo digital para los países emergentes. Si bien consideran que la "soberanía de los datos" es ilusoria ya que el partido-Estado chino retiene el control sobre las empresas chinas que suministran infraestructura digital e instan al desarrollo de infraestructuras legales acordes con las estrategias de desarrollo digital.

[14] P. M. Schwartz, "Global Data Privacy: The EU Way", *New York University Law Review*, vol. 94, 2019, pp. 771-818.

[15] N. Purtova, "The Law of Everything. Broad concept of Personal Data and Future of EU Data Protection Law", *Innovation and Technology*, Vol. 10, nº 1, 2018, pp. 40-81, p. 77; D. Erdos, *The UK and the EU Personal Data Framework After Brexit: Another Switzerland?*, University of Cambridge Faculty of Law Research Paper No. 15/2021, p. 17; y A. Chander, M. Abraham, S. Chandy Y. Fang, D. Park e I. Yu, *Achieving Privacy. Costs of Compliance and Enforcement of Data Protection Regulation*, World Development Report 2021 Background Paper, World Bank Group, 2021. Disponible en: https://openknowledge.worldbank.org/bitstream/handle/10986/35306/Achieving-Privacy-Costs-of-Compliance-and-Enforcement-of-Data-Protection-Regulation.pdf?sequence=1

[16] Véase United States Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers*, 2021. Disponible en: https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf Cabe señalar que el resto de iniciativas legislativas de la Comisión estudiadas en este trabajo también son consideradas una barrera al comercio por los Estados Unidos incluso antes de entrar en vigor. Estados Unidos se ha mostrado partidario hasta el momento de no regular a los intermediarios tecnológicos para beneficiar a sus grandes multinacionales, no obstante, es posible que esta aproximación cambie parcialmente bajo la administración Biden.

[17] Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo "Una nueva agenda UE-EE.UU. para el cambio global", JOIN/2020/22 final.

[18] K. Bhatia, "The U.S. and Europe should launch a trade and technology council", *Google Blog,* 9/4/2021. Disponible en: https://blog.google/outreach-initiatives/public-policy/us-europe-technology-trade-council

**5**. En cualquier caso, la Comisión Europea en su informe sobre la aplicación del RGPD dos años después de que se empezará a aplicar considera esta norma un claro éxito.[19] Por ello, la Comisión ha utilizado el RGPD como una especie de modelo cuyos elementos parcialmente replica en la adopción de posteriores propuestas legislativas que buscan completar el Mercado Único Digital[20] y avanzar en la consecución de un futuro digital para Europa[21], sobre todo a partir de 2017.

**6**. Papakonstantinou y De Hert consideran que el RGPD sigue el siguiente esquema: se basa en un conjunto de términos únicos y especializados,[22] un conjunto de principios básicos (como la limitación de la finalidad o la minimización de los datos) y derechos específicos (como los de información, acceso y rectificación) con la supervisión de una agencia pública especializada. Así, observan una mimesis que reviste tres formas respecto a la propuesta de Ley de Gobernanza de Datos (*Data Governance Act*, conocida como DGA por sus siglas en inglés),[23] en lo relativo a las definiciones, la sustancia (principios y derechos) y las instituciones (con la creación del Comité Europeo de Innovación en materia de Datos).[24] Los autores ven muestras de estos tipos de mimetismo también en la propuesta del Parlamento Europeo para regular la inteligencia artificial.[25] Sin embargo, consideran que esta réplica del modelo del RGPD no se ha dado en las propuestas de Ley de Servicios Digitales (*Digital Services Act*, conocida como DSA por sus siglas en inglés)[26] y la Ley de Mercados Digitales (*Digital Markets Act*, conocida como DMA por sus siglas en inglés).[27]

**7.** Sin embargo, en este artículo prestaremos atención a otros elementos del RGPD, aquellos de naturaleza más procesal e institucional[28] que buscan mejorar el cumplimiento de esta norma a pesar de los retos añadidos de referirse a un ámbito digital en el que muchos de los destinatarios de la norma se encuentran localizados fuera del Espacio Económico Europeo. Así veremos que por su propia naturaleza la DGA tendrá pocos puntos en común con el RGPD en este sentido, pero, sin embargo, la DSA y la DMA van a tener muchos y resulta evidente la influencia del RGPD sobre ellas.

**8.** En este artículo estudiaremos algunos de los elementos clave en ese sentido del RGPD: su naturaleza de reglamento, la aplicación extraterritorial, la obligación de que algunas empresas localizadas fuera de la UE nombren a un representante dentro de la misma, la necesidad de autoridades independientes de control en cada Estado miembro para vigilar su aplicación que se agrupan en un comité europeo y las multas elevadas por su incumplimiento.

---

[19] Comunicación de la Comisión al Parlamento Europeo y al Consejo "La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos", COM/2020/264 final.

[20] Véase Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Estrategia para el Mercado Único Digital de Europa", COM/2015/0192 final.

[21] Véase Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Configurar el futuro digital de Europa", COM/2020/67 final.

[22] Como interesado (*data subject*), responsable del tratamiento (*controller*) o encargado del tratamiento (*processor*).

[23] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM/2020/767 final.

[24] Véase V. Papakonstantinou y P. De Hert, "Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI", *European Law Blog*, 1/4/2021. Disponible en: https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/

[25] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas. Véase V. Papakonstantinou y P. De Hert, "Refusing to award legal personality to AI: Why the European Parliament got it wrong", *European Law Blog*, 25/11/2020. Disponible en: https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/

[26] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE, COM/2020/825 final.

[27] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales), COM/2020/842 final.

[28] Esta aproximación no coincidiría con la mimesis de definiciones o sustancial, pero sí parcialmente con la institucional.

**9.** En particular, analizaremos cómo se han replicado estos elementos en las propuestas de Reglamento sobre la privacidad y las comunicaciones electrónicas (conocido como Reglamento e-privacy),[29] el Reglamento de las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (conocidas por sus siglas en inglés EPOC),[30] el Reglamento para la prevención de la difusión de contenidos terroristas en línea (conocido como TERREG),[31] la DSA, la DMA y la *Artificial Intelligence Act* (AIA).[32]

**10.** De Gregorio considera el RGPD como el primer instrumento que marcó un cambio de tendencia en la UE hacia un constitucionalismo digital al que se llegaría tras una primera fase de liberalismo digital y una segunda en la que destacaría el activismo judicial. Así esta tercera fase buscaría asumir lo ya apuntado por el TJUE en su jurisprudencia y regular a los intermediarios de una manera más estricta para proteger los derechos de los usuarios.[33] El primer paso sería el RGPD y después el resto de iniciativas comentadas como el Reglamento TERREG o la DSA, por lo que no es de extrañar que el RGPD haya tenido una fuerte impronta en estas propuestas de normas.

## II. Elementos replicados

### 1. De directivas a reglamentos y a ¿leyes?

**11.** En el Derecho de la UE encontramos diferentes tipos de normas con características distintas. En la mayoría de los casos, los tratados prevén el tipo de acto que debe utilizarse dependiendo de la materia. De forma excepcional, el artículo 296 del Tratado de Funcionamiento de la Unión Europea

[29] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM/2017/010 final.

[30] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM/2018/225 final.

[31] Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea Contribución de la Comisión Europea a la reunión de los dirigentes de Salzburgo los días 19 y 20 de septiembre de 2018, COM/2018/640 final.

[32] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión, COM/2021/206 final.

Sin ser el objeto de este artículo puede destacarse que una de las críticas hechas a la propuesta de la Comisión Europea es que a diferencia del RGPD no ofrece recursos individuales o colectivos a las personas que hayan sufrido daños causados por un incumplimiento de la AIA. Esto se ha criticado por no poner a las personas en el primer plano del reglamento, véase F. Reinhold y A. Müller "AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps", *AlgorithmWatch,* 2021. Disponible en: https://algorithmwatch.org/en/wp-content/uploads/2021/04/AWs-response-on-ECs-AI-regulation-proposal-April-2021-v1-2021-04-21.pdf En ese caso la Comisión justifica esta diferencia en el sentido de que lo que han intentado no es crear nuevos recursos sino hacer más eficientes los ya existentes, por ejemplo, en el ámbito de la discriminación. Véase la intervención de Killian Gross, Jefe de Unidad de Inteligencia Artificial e Industria Digital de la Dirección General de Redes de Comunicación, Contenido y Tecnologías de la Comisión Europea en el Webinar "Towards a European AI Regulation" organizado por AI4Belgium el 18 de mayo de 2021. Disponible en: https://www.youtube.com/watch?v=pumw6QOwOBs

A diferencia de las otras propuestas analizadas en este artículo la AIA no busca regular a los intermediarios de Internet, pero se ha elegido porque también es una norma muy importante del mercado único digital, incluso se le ha tildado de ser el nuevo "RGPD para la Inteligencia Artificial".

Además, la inteligencia artificial como servicio desempeñará un papel cada vez más importante en la infraestructura técnica de la sociedad, permitiendo, facilitando y respaldando la funcionalidad de muchas aplicaciones. Véase J. Cobbe y J. Singh, "Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges", *Computer Law & Security Review*, 2021 http://dx.doi.org/10.2139/ssrn.3824736

[33] G. De Gregorio, "The rise of digital constitutionalism in the European Union", *International Journal of Constitutional Law*, vol. 19, nº 1, 2021, pp. 41–70, https://doi.org/10.1093/icon/moab001 y del mismo autor "The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism", *Diritti Comparati,* 17/05/2021. Disponible en: https://www.diritticomparati.it/the-digital-services-act-a-paradigmatic-example-of-european-digital-constitutionalism/

(TFUE) permite a las instituciones decidir el tipo de acto que debe adoptarse en cada caso teniendo en cuenta el principio de proporcionalidad. Según el artículo 288 TFUE, para ejercer las competencias de la UE, las instituciones adoptarán reglamentos, directivas, decisiones, recomendaciones y dictámenes. El reglamento tendrá un alcance general, será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro, mientras que la directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.

**12**. En muchos casos la Comisión puede optar entre proponer una directiva o un reglamento. Tradicionalmente en las propuestas en el ámbito digital optaba por usar directivas, un ejemplo paradigmático es el de la Directiva de protección de datos personales de 1995.[34] En el momento en que se hizo perentoria su modernización, la Comisión optó por proponer su sustitución por un reglamento por considerarlo el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la UE. En su opinión, la aplicabilidad directa de un reglamento reduciría la fragmentación jurídica y ofrecería una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior.[35] Aun así el Consejo, la institución formada por los representantes de los Estados miembros, incluyó en el texto final del RGPD en su considerando 10 el reconocimiento de un margen de maniobra para que los Estados miembros especificaran sus normas, inclusive para el tratamiento de categorías especiales de datos.

**13.** Además, la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos pasó a regularse por una Directiva[36] para garantizar en este ámbito la armonización a nivel de la UE y dejar, al mismo tiempo, a los Estados miembros la flexibilidad necesaria a la hora de aplicar los principios, las normas y sus exenciones a nivel nacional.[37] En este sentido, cabe la pena recordar la transposición tardía de esta Directiva por parte de España, lo que le supuso una condena por parte del TJUE en la que se le impuso el abono de una suma a tanto alzado de 15 000 000 euros y una multa coercitiva diaria de 89 000 euros hasta que adoptó la norma de transposición.[38]

**14.** En el mismo sentido, a la hora de actualizar la Directiva de e-privacy,[39] la Comisión también optó por proponer un reglamento para garantizar la coherencia con el RGPD (aunque en opinión de la autora para eso no fuera necesario un reglamento) y ofrecer seguridad jurídica a usuarios y empresas evitando interpretaciones divergentes en los Estados miembros. Un reglamento, según la Comisión, garanti-

[34] 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, *DOUE* L 281 de 23 de noviembre de 1995, p. 31.

[35] Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), COM/2012/011 final, p. 6.

[36] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, *DOUE* L 119 de 4 de mayo de 2016, p. 89.

[37] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, COM/2012/010 final, p. 6.

[38] STJUE 25 de febrero de 2021, *Comisión Europea c. Reino de España*, C-658/19, ECLI:EU:C:2021:138.

[39] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), *DOUE* L 201 de 31 de julio de 2002, p. 37.

zaría un nivel uniforme de protección de los usuarios en toda la UE y abarataría los costes de conformidad de las empresas que desarrollan actividades transfronterizas.[40] Como muchas empresas tecnológicas tienen la capacidad de ofrecer sus servicios en varios países europeos, tener que cumplir una única norma les permite economías de escala. Estas razones se han constituido en un elemento que ha fomentado la adopción de reglamentos en este ámbito, junto con la necesidad de evitar la fragmentación del mercado único.

**15.** Las ordenes de investigación europeas están reguladas en una directiva[41], lo cual es lo normal en los instrumentos de reconocimiento mutuo en el ámbito del Espacio de Libertad, Seguridad y Justicia, dado que proviene de un ámbito intergubernamental que se regía por reglas diferentes como era la cooperación judicial y policial en materia penal que se instrumentalizaba en gran medida a través de decisiones marco. Sin embargo, a la hora de regular las ordenes de entrega y conservación de pruebas electrónicas, la Comisión propuso hacerlo a través de un reglamento porque la propuesta se refería a procedimientos transfronterizos para los que se requerían normas uniformes y, por tanto, en su opinión, no era necesario dejar un margen a los Estados miembros para transponer dichas normas. Argumentó que un reglamento es directamente aplicable, aporta claridad y más seguridad jurídica y evita interpretaciones divergentes en los Estados miembros y otros problemas de transposición que han padecido las Decisiones marco relativas al reconocimiento mutuo de las sentencias y resoluciones judiciales. Además, un reglamento permite imponer las mismas obligaciones de manera uniforme en toda la UE.[42] Algo muy parecido ocurrió con el Reglamento TERREG.

**16.** Así podemos ver como la Comisión ha optado por reglamentos en la mayoría de nuevas iniciativas presentadas en el marco del mercado único digital.[43] Esto se ve además acompañado de una nueva tendencia sobre todo a partir de 2020 de bautizar a estas normas como *Act* (o ley en español), así encontramos la *Digital Services Act* (Ley de Servicios Digitales), la *Digital Markets Act* (Ley de Mercados Digitales), la *Data Governance Act* (Ley de Gobernanza de Datos), y la *Artificial Intelligence Act* (Ley de Inteligencia Artificial).[44] Cabe aclarar que a nivel de la UE no existen normas que sean propiamente "leyes", sino que son realmente reglamentos.[45] No obstante, la propia UE está usando en los últimos años el término inglés *Act* para referirse de manera abreviada a algunas de sus normas más importantes e incluyéndolo en el título de las mismas, convirtiéndolo así en la abreviatura oficial.[46] Pro-

[40] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM/2017/010 final, p. 6.

[41] Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, *DOUE* L 130 de 1 de mayo de 2014, p. 1.

[42] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM/2018/225 final, p. 6. Si bien en relación a las normas armonizadas para la designación de representantes legales a efectos de recabar estas pruebas para procesos penales, la Comisión propuso una directiva. Véase Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, COM/2018/226 final.

[43] Si bien podemos encontrar algunas excepciones, por ejemplo, a la hora de adaptar la modernización del régimen de la protección de los derechos de autor, la Comisión siguió apostando por una directiva para dejar cierto margen de maniobra a los Estados. Esto daría lugar a 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, *DOUE* L 130 de 17 de mayo de 2019, p. 92.

[44] El único ejemplo que rompe esta tendencia de traducción es la *Cybersecurity Act* que se ha traducido al español como Reglamento sobre la Ciberseguridad. Véase Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»), *DOUE* L 151 de 7 de junio de 2019, p. 15.

[45] Esto es lo habitual, pero no es siempre el caso, así la que se conoce como *European Accesibility Act* es en realidad la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios, *DOUE* L 151 de 7 de junio de 2019, p. 70.

[46] Sobre esta tendencia, véase V. Papakonstantinou, "The "act-ification" of EU law: The (long-overdue) move towards "eponymous" EU legislation", *European Law Blog*, 26/1/2021. Disponible en: https://europeanlawblog.eu/2021/01/26/the-act-ification-of-eu-law-the-long-overdue-move-towards-eponymous-eu-legislation/

blemente se trata de una manera de conseguir nombres más cortos y "pegadizos" (aunque al RGPD le bastaron con sus siglas, también muy conocidas en inglés como GDPR) que puedan ser entendidos mejor por las personas no familiarizadas con los diferentes tipos de normas europeas.[47] No obstante, esta tipología también podría llevar a nuevas confusiones.

## 2. Aplicación extraterritorial

**17.** Según el artículo 3 del RGPD, éste se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la misma o no. Pero lo que es más interesante es que también se aplica al tratamiento de datos personales de interesados que residan en la UE por parte de un responsable o encargado no establecido en la misma, cuando las actividades de tratamiento estén relacionadas con: la oferta de bienes o servicios a dichos interesados en la UE, independientemente de si a estos se les requiere su pago,[48] o el control de su comportamiento, en la medida en que este tenga lugar en la UE.[49] Como podemos ver, la primera parte sigue un principio de territorialidad subjetiva, teniendo en cuenta quién procesa o controla los datos, mientras que la segunda agrega un principio de personalidad pasiva siguiendo al destinatario de tales acciones.

**18.** El objetivo de este amplio ámbito territorial es que la protección que ofrece el RGPD "viaje" con los datos personales allá donde vayan en una sociedad globalizada donde los datos cruzan fronteras con un simple clic. La UE se guía por el razonamiento de que ofrecer protección solo para el procesamiento de datos que tiene lugar dentro de las fronteras europeas no sería suficiente. Esta medida también busca ofrecer igualdad de condiciones para las empresas europeas sin crear una regulación más estricta que supusiera cargas solo para ellas. La aplicación extraterritorial del RGPD significa que cualquier empresa que desee acceder al mercado europeo para ofrecer sus servicios y bienes y tratar datos personales "europeos" en el proceso debe cumplir con estas reglas aunque tenga su sede en un tercer país.[50] La aplicación extraterritorial de la legislación no es algo nuevo,[51] pero sí que se puede ver que está cobrando mucha fuerza en los aspectos relativos a la regulación de Internet.[52] Frosio considera que

[47] En este sentido se puede recodar que el art. I-33 del descartado Tratado por el que se establecía una Constitución para Europa sustituía dentro de los actos jurídicos de la UE la denominación de reglamento por ley europea y la de directiva por ley marco europea.

[48] Según el considerando 23 del RGPD, para determinar si el responsable o encargado ofrece bienes o servicios a interesados que residan en la UE, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la UE. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la UE, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la UE, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la UE.

[49] Según el considerando 24 del RGPD, para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en Internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

[50] Véase A. Gascón Marcén, "The extraterritorial application of European Union Data Protection Law", *Spanish Yearbook of International Law*, Nº 23, 2019, pp. 413-425, p. 415.

[51] Véase R. Dover y J. Frosini, *The Extraterritorial Effects of Legislation and Policies in the EU and US* (European Union, Brussels, 2012) [doi: 10.2861/75161]. Según Gallego, a pesar de que la UE nunca ha sido una completa defensora de la extraterritorialidad, comienza a redoblar su ejercicio a través de la extensión territorial, la cual permite controlar aquellas conductas que, aunque se lleven a cabo en el extranjero, repercutan en los intereses generales de la UE. Véase A. C. Gallego Hernández, "La aplicación de la extensión territorial del Derecho de la Unión Europea", *Cuadernos Europeos de Deusto,* n.º 63 (septiembre), 2020, pp. 297-313. https://doi.org/10.18543/ced-63-2020pp297-313.

[52] Véase Internet Society, *The Internet and extra-territorial effects of laws,* Internet Society, 2018, p. 1. Esta organización advierte que muchos Estados están imponiendo reglas que se extienden a Internet en otros lugares, obstaculizan la innovación,

la aplicación extraterritorial global de derechos diversos ha surgido como una tendencia constante en la reciente regulación en línea, tanto a nivel internacional como de la UE.[53]

**19**. Sin embargo, el RGPD ha sido duramente criticado porque, con la cantidad de empresas que se encuadran en estos criterios en todo el mundo, es más fácil para las multinacionales adaptarse a él mientras que es muy costoso para las pequeñas y medianas empresas.[54] Además, las autoridades de protección de datos (APD) en los Estados miembros tienen recursos limitados, por lo que Svantesson argumenta que, como habrá más empresas extranjeras que no cumplan con el RGPD que recursos para investigarlas, la aplicación real del mismo necesariamente será arbitraria, lo que socavaría la legitimidad de cualquier acción de ejecución que se adopte.[55] Sin embargo, Azzi considera legítima esta aplicación extraterritorial y argumenta que la UE está equipada con las herramientas relevantes para hacer cumplir el RGPD en el exterior, aunque haya que desarrollarlas más.[56] Hert y Czerniawski añaden que este enfoque, aunque no sin inconvenientes y desafíos para los intereses estatales y los derechos individuales, resuelve uno de los mayores problemas a los que se enfrentaba hasta entonces la normativa europea de protección de datos, que era la falta de jurisdicción sobre los responsables del procesamiento de datos en terceros países que afectaban a un número considerable de datos de europeos.[57]

**20.** Los legisladores europeos eran bastante conscientes de que la aplicación extraterritorial de las leyes podía tener impactos indeseables. El propio RGPD en su considerando 115 establece que la aplicación extraterritorial de algunas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la UE en virtud del RGPD, y, por tanto, las transferencias de datos sólo deben hacerse respectando las condiciones del mismo. Así vemos que el RGPD establece su propia aplicación extraterritorial, pero excluye la de las leyes extranjeras en muchos casos. Un conflicto de esta naturaleza puede darse, por ejemplo, cuando las autoridades estadounidenses requieran datos en el marco de una investigación penal a una compañía situada en su territorio pero que sean referentes a un residente de la UE en contra de lo establecido en el RGPD, por lo que la empresa puede encontrarse con obligaciones legales contradictorias.[58]

**21.** China ha adoptado una norma en 2021 para limitar los efectos en sus empresas de la aplicación extraterritorial por parte de otros países de sus leyes y reaccionar a las mismas, se trata de la *Order No. 1 of 2021 on Rules on counteracting unjustified extra-territorial application of foreign legislation and other measures*.[59] Es una clara respuesta a determinadas sanciones impuestas por Estados Unidos a las empresas chinas, sin embargo, podría aplicarse también como resultado de las normas europeas

disuaden la inversión en sus propios países y corren el riesgo de crear nuevas brechas digitales que perjudiquen a sus propios ciudadanos.

[53] G. Frosio, "Enforcement of European Rights on a Global Scale", en E. Rosati (ed.), *Handbook of European Copyright Law,* Routledge, 2021.

[54] Véase M. Scott, L. Cerulus y L. Kayali "Six months in, Europe's privacy revolution favors Google, Facebook", *Politico.eu*, 23/11/2018. Disponible en: https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/ o M. Scott, L. Cerulus y S. Overly, "How Silicon Valley gamed Europe's privacy rules", *Politico.eu,* 22/5/2019. Disponible en: https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/

[55] D. J. B. Svantesson, "European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments", *Journal of Intellectual Property, Information Technology and E-Commerce Law,* vol. 9, nº 2, 2018, pp. 113-125, p. 118.

[56] A. Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 9, nº 2, 2018, pp. 126-137, p. 137.

[57] P. de Hert y M. Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the General Data. Protection Regulation in its wider context", *International Data Privacy Law*, vol. 6, nº 3, 2016, pp. 230-243, p. 230, doi:10.1093/idpl/ipw008.

[58] Véase *EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection* de 2019. Para solucionar este problema Estados Unidos y la UE se encuentran actualmente negociando un acuerdo sobre el acceso transfronterizo a pruebas electrónicas para la cooperación judicial en materia penal.

[59] Disponible su traducción al inglés en:
http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml

porque sus definiciones son bastante amplias. No obstante, uno de los requisitos de esta orden es que la aplicación extraterritorial se haga en violación del Derecho internacional, lo que en principio no sería el caso, pero dependería de la interpretación que hagan los tribunales chinos.[60] En definitiva, podemos ver dos claras tendencias mundiales: la aplicación de las normas de manera extraterritorial y la resistencia y problemas que esto puede crear.

**22.** Los problemas son múltiples y los críticos tienen buenas razones para estar preocupados, pero la dificultad para garantizar la aplicación del RGPD o la falta de recursos para ello no pueden hacer que apuntemos a estándares más bajos de protección de los derechos fundamentales.[61] Sobre todo teniendo en cuenta cómo el RGPD ha servido para elevar este nivel de protección no sólo en Europa. Al final la Comisión ha buscado solucionar un problema que viene definido por la actuación transfronteriza de los intermediarios que busca regular situados normalmente fuera de las fronteras europeas, pero con un fuerte impacto sobre sus ciudadanos. Se quiere hacer frente a lo que Hilldebrandt ha bautizado como "brute jurisdiction" de facto de algunos intermediarios que se basa en la fuerza normativa de control sobre las nuevas infraestructuras de comunicaciones (de ahí la cada vez más famosa definición como *gatekeepers*) y frente a la que llama a repensar los instrumentos que el derecho utiliza para garantizar el imperio de la ley.[62]

**23.** Así, tiene sentido que cuando la Comisión propuso el Reglamento e-privacy, eligiera seguir en esta línea y no fijarse en dónde estaban situados los servicios de comunicaciones electrónicas sino los destinatarios, porque, según su artículo 3, el Reglamento se aplicará a la prestación de servicios de comunicaciones electrónicas a los usuarios finales en la UE, independientemente de si el usuario final tiene que pagar por ellos; a la utilización de dichos servicios; y a la protección de la información relativa a los equipos terminales de los usuarios finales situados en la UE.[63]

**24**. El artículo 3 de la propuesta de Reglamento EPOC también establece que éste se aplicará a los proveedores que ofrezcan servicios en la UE. En su considerando 28 aclara, no obstante, que una estrecha vinculación con la UE es necesaria para determinar el ámbito de aplicación del mismo y sigue los parámetros establecidos en el RGPD, aunque añade nuevos criterios como que la orientación de las actividades hacia un Estado miembro también puede derivarse de la disponibilidad de una aplicación para móvil en la tienda de aplicaciones nacional. En opinión de algunos autores como Svantesson, que ya dudaban de que el RGPD estableciera un criterio que mostrará una estrecha vinculación, este Reglamento a pesar del primer inciso tampoco lo consigue en la práctica.[64]

**25.** La *CLOUD Act* estadounidense que también busca facilitar el acceso a pruebas electrónicas para investigaciones penales tomó como punto de conexión el contrario ya que sirve para obligar a las

[60] Véase D. J. B. Svantesson, "How will China's new 'extraterritoriality shield' affect the Internet?" *Linkedin*, 22/01/2021. Disponible en: https://www.linkedin.com/pulse/how-chinas-new-extraterritoriality-shield-affect-svantesson

[61] El art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce la protección de los datos personales como un derecho fundamental.

[62] M. Hildebrandt, "Text-Driven Jurisdiction in Cyberspace", Keynote Hart Workshop 26-28 April 2021. New Perspectives on Jurisdiction and the Criminal Law. Disponible en: https://osf.io/jgs9n/

[63] El Reglamento e-privacy es una propuesta de legislación controvertida, porque si bien existía consenso sobre la necesidad de actualizar la Directiva de e-privacy no sobre cómo hacerlo, véase A. Gascón Marcén, *El Reglamento sobre la privacidad y las comunicaciones electrónicas, la asignatura pendiente del Mercado Único Digital*, Documento de Trabajo Número 93/2020, Serie Unión Europea y Relaciones Internacionales, Real Instituto Universitario de Estudios Europeos, Universidad CEU San Pablo, 2020. Disponible en: https://repositorioinstitucional.ceu.es/bitstream/10637/10812/1/reglamento_gascon_2020.pdf Así el Parlamento Europeo adoptó muy rápido su mandato para negociar en el trílogo con el Consejo de la UE, pero al Consejo le costó cuatro años hacerlo por el fuerte disenso a nivel interno. Además, el Consejo sólo lo consiguió insertando una mención a la conservación de datos que podría entrar en conflicto con la jurisprudencia del Tribunal de Justicia de la Unión Europea y, además, modificó determinados apartados que pueden suponer un conflicto con las disposiciones del RGPD, véase EDPB, *Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021*.

[64] D. J. B. Svantesson, "European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments", 9 (2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2018), 113-125, p. 120.

compañías localizadas en Estados Unidos a entregar esas pruebas a las autoridades independientemente de dónde se encuentren los datos, suponiendo así una aplicación extraterritorial diferente. La cuestión es que muchas compañías tecnológicas están establecidas en Estados Unidos así si la UE quiere facilitar el acceso a esos datos debe optar por un punto de conexión diferente como lo ha hecho.[65]

**26.** El artículo 1.2 de la propuesta de Reglamento para la prevención de la difusión de contenidos terroristas establece que será de aplicación a los prestadores de servicios de alojamiento de datos que ofrecen servicios en la UE, independientemente de su lugar de establecimiento principal. Esta propuesta de Reglamento fue bastante controvertida y recibió críticas por múltiples razones,[66] las modificaciones a las que fue sometida en el marco de las negociaciones del trílogo entre el Consejo de la UE, y el Parlamento Europeo, la mejoraron sensiblemente,[67] aunque algunos elementos todavía deberían haber sido reformados para convertirla en una norma garantista de los derechos humanos.[68]

**27.** Varias organizaciones no gubernamentales que luchan por la protección de los derechos humanos de los usuarios de Internet pidieron en una carta conjunta a los Estados miembros de la UE que respetaran los principios de territorialidad y garantizaran el acceso a la justicia en casos de retirada transfronteriza asegurándose de que solo el Estado miembro en el que el proveedor de servicios de alojamiento tiene su establecimiento legal pueda emitir órdenes de retirada.[69] No obstante, esto iba totalmente en contra del objetivo de la norma que buscaba facilitar la creación de órdenes transfronterizas de retirada por lo que el Consejo de la UE ignoró esta petición. Sin embargo, es relevante tener en cuenta que este tipo de mecanismos puede ser utilizado en otras jurisdicciones por gobiernos autoritarios para fomentar

[65] Véase R. López Jiménez, "El nuevo marco jurídico transfronterizo de las pruebas electrónicas las órdenes de entrega y conservación de las pruebas electrónicas", *Revista General de Derecho Europeo*, nº. 49, 2019; L. Gómez Amigo, "Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima", *Revista Española de Derecho Europeo,* nº. 71, 2019, pp. 23-55; A. Gascón Marcén, "Las órdenes europeas de entrega y conservación de pruebas electrónicas: Evaluación de la propuesta de la Comisión Europea", *El mercado único en la Unión Europea: balance y perspectivas jurídico-políticas*, Dykinson, 2019 y de la misma autora, "Improving access to electronic evidence: the European normative struggle", *Cybercrime: new threats, new responses*, Huygens Editorial, 2020, pp. 140-157.

En el mismo sentido, aunque de manera menos ambiciosa parece ir orientado el segundo protocolo del Convenio de Budapest sobre la Ciberdelincuencia que establecerá que cada Estado parte tomará medidas legislativas y de otro índole que sean necesarias para facultar a sus autoridades competentes a emitir una orden que se enviará directamente a un proveedor de servicios en el territorio de otra Parte, con el fin de obtener la divulgación de información especificada y almacenada del suscriptor en posesión o control de ese proveedor de servicios, cuando la información del suscriptor sea necesaria para las investigaciones o procedimientos penales específicos en la Parte emisora. Véase Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Draft Protocol version 3, T-CY (2020)7. Disponible en: https://rm.coe.int/0900001680a2aa1c

[66] Véase A. Kuczerawy, *The Proposed Regulation on Preventing the Dissemination of Terrorist Content Online: Safeguards and Risks for Freedom of Expression*, Center for Democracy and Technology, 2018. Disponible en: https://cdt.org/wp-content/uploads/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf; Opinion of European Union Agency for Fundamental Rights 2/2019 on the Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications, 12 de febrero de 2019; y Carta del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, el Relator Especial sobre el derecho a la privacidad y el Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo sobre la propuesta de Reglamento sobre la prevención de la difusión de contenidos terroristas del 7 de diciembre de 2018 (OL OTH 71/2018). Disponible en: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234

[67] Véase Comunicación de la Comisión al Parlamento Europeo con arreglo al artículo 294, apartado 6, del Tratado de Funcionamiento de la Unión Europea sobre la posición del Consejo sobre la adopción de un Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea, COM/2021/123 final, y J. C. York y C. Schmon "The EU Online Terrorism Regulation: a Bad Deal", *Electronic Frontier Foundation*, 7/4/2021. Disponible en: https://www.eff.org/deeplinks/2021/04/eu-online-terrorism-regulation-bad-deal

[68] Véase Carta conjunta de una serie de organizaciones en pro de los derechos humanos de los usuarios de Internet a los miembros del Parlamento Europeo de 25 de marzo de 2021. Disponible en : https://edri.org/wp-content/uploads/2021/03/MEP_TERREG_Letter_EN.pdf

[69] Véase Carta conjunta de una serie de organizaciones en pro de los derechos humanos de los usuarios de Internet a los Estados miembros en el marco del Consejo de la UE de 27 de marzo de 2020. Disponible en: https://edri.org/wp-content/uploads/2020/03/Final-PDF-Letter-TERREG2.pdf

la censura como ya se ha puesto de manifiesto,[70] sobre todo si se hace una definición muy amplia de lo que son contenidos terroristas. Por ello, en este tipo de iniciativas es importante crear salvaguardas para los derechos, por ejemplo, en este caso sería positivo que el país afectado donde vive la persona o del que es nacional pudiera objetar la aplicación de la orden.[71]

**28**. La propuesta de DSA, según su artículo 1.3, también se aplicará a los servicios intermediarios prestados a destinatarios del servicio que tengan su lugar de establecimiento o residencia en la UE, con independencia del lugar de establecimiento de los prestadores de dichos servicios, y la propuesta de DMA se aplicará a los servicios básicos de plataforma prestados u ofrecidos por guardianes de acceso a usuarios profesionales establecidos en la UE o usuarios finales establecidos o situados en la UE, independientemente del lugar de establecimiento o residencia de los guardianes de acceso y de la ley aplicable a la prestación del servicio.

**29**. La aplicación extraterritorial ha claramente inspirado la propuesta de AIA, porque ésta según su artículo 2.1 se aplicará a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la UE, con independencia de si dichos proveedores están establecidos en la UE o en un tercer país; los usuarios de sistemas de IA que se encuentren en la UE; y los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la UE.[72] Es decir que la aplicación a los proveedores se desgaja totalmente de la cuestión de dónde estén situados, lo importante es que introduzcan sus sistemas en la UE, o incluso que sin hacerlo los resultados de esos sistemas se usen en la UE.

**30**. Se puede observar que existe un modelo que se va adaptando para la normativa relativa a los intermediarios de Internet que toma como punto de conexión que el destinatario del servicio esté en la UE, independientemente de la localización del propio intermediario. Esto supondrá la aplicación extraterritorial de todas estas normas para proteger mejor a los europeos, pero con los conflictos que hemos visto que esto puede crear.

### 3. Designación de un representante en uno de los Estados miembros

**31.** Para asegurarse de que las compañías localizadas fuera de la UE que quedan obligadas por el RGPD cumplan el mismo, éstas deben nombrar un representante en uno de los Estados miembros de

[70] En el marco de la discusión sobre un posible derecho al olvido, el Abogado General Niilo Jääskinen destacó como "Internet ha revolucionado el acceso a todo tipo de información y su difusión, y ha puesto en marcha nuevos medios de comunicación y de interacción social entre particulares" y a su juicio "el derecho fundamental a la información merece protección particular en Derecho de la Unión Europea, particularmente a la luz de la tendencia cada vez mayor de los regímenes autoritarios en todo el mundo a limitar el acceso a Internet o a censurar el contenido disponible en él." Conclusiones del Abogado General ante el TJUE Niilo Jääskinen presentadas el 25 de junio de 2013, C-131/12, *Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, párr. 121.

[71] Véase T. Christakis, "Lost in notification? Protective logic as compared to efficiency in the European Parliament's E-Evidence Draft Report", *Cross-Border Data Forum*, 7/1/2020. Disponible en: https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/

[72] En su considerando 11 la propuesta aclara que "Debido a su carácter digital, algunos sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento aunque no se introduzcan en el mercado, se pongan en servicio ni se utilicen en la Unión. Tal es el caso, por ejemplo, de un operador establecido en la Unión que contrate determinados servicios a otro operador establecido fuera de la Unión en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo y que tiene repercusiones para las personas físicas ubicadas en la Unión. En dichas circunstancias, el sistema de IA usado por el operador de fuera de la Unión podría tratar datos recabados legalmente en la UE y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión la información de salida generada por dicho sistema de IA a raíz de su tratamiento, sin que el sistema de IA en cuestión se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar la elusión de este Reglamento y asegurar la protección efectiva de las personas físicas ubicadas en la Unión, el presente Reglamento también debe aplicarse a los proveedores y usuarios de sistemas de IA establecidos en un tercer país, en la medida en que la información de salida generada por dichos sistemas se utilice en la Unión."

la UE en que estén los interesados cuyos datos personales se traten, conforme al artículo 27 del RGPD. Si bien teniendo en cuenta la onerosidad de esta obligación, ésta se matiza porque no será aplicable al tratamiento que sea ocasional, que no incluya el manejo a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o a las autoridades u organismos públicos. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento.

**32.** Esta obligación resulta onerosa para las compañías extranjeras que sino no tendrían presencia física en la UE, sobre todo para las pequeñas y medianas empresas.[73] No obstante, es una manera efectiva de asegurar el cumplimiento y, en realidad, se trata de nombrar un único representante para 27 Estados. El problema es que este requerimiento está siendo imitado en las normativas de protección de datos de muchos otros países, lo que lo convierte en requisito cada vez más costoso para las empresas que tienen que multiplicar sus representantes por todo el mundo. Desgraciadamente algunos Estados están exigiendo la presencia de un representante de los intermediarios de Internet en su territorio para hacerles cumplir normas que pueden violar los derechos humanos al vulnerar la libertad de expresión y facilitar la censura.[74]

**33.** Es extremadamente poco usual que se establezcan multas por falta de un representante dado que la mayoría de los casos en los que las agencias de protección de datos se fijan en la actuación de empresas de fuera de la UE, éstas suelen ser bastante grandes y, por tanto, están representadas en la misma. No obstante, se están empezando a imponer sanciones por falta de cumplimiento de esta obligación. Un ejemplo sería la multa que la Agencia holandesa de protección de datos impuso a LocateFamily.com con una suma a tanto alzado de 525,000 euros y una multa coercitiva de 20,000 por cada dos semanas en las que todavía no se nombrara a dicho representante con un montante máximo de 120,000 euros.[75]

**34.** En el art. 3 de la propuesta de Reglamento e-privacy, se establece que el proveedor de un servicio de comunicaciones electrónicas que no esté establecido en la UE deberá designar por escrito a un representante en la misma. El representante estará establecido en uno de los Estados miembros en que estén situados los usuarios finales de esos servicios y facultado para responder a preguntas y facilitar información que complemente o supla la del proveedor al que representa, en particular a las autoridades de control y los usuarios finales, sobre todos los asuntos relativos al tratamiento de datos de comunicaciones electrónicas a fin de garantizar el cumplimiento del presente Reglamento.

**35.** Según el art. 7 del Reglamento EPOC, las órdenes europeas de entrega y de conservación de pruebas electrónicas deberán remitirse directamente al representante legal designado por el proveedor de servicios a efectos de recabar pruebas para procesos penales.[76] Éste se encargará de la recepción, el cumplimiento y la ejecución de las resoluciones y órdenes emitidas por las autoridades competentes de los Estados miembros a efectos de recabar pruebas para procesos penales. En este Reglamento, la figura del representante es muy importante porque sirve para centralizar la gestión de este tipo de órdenes y hacerlas más efectivas, incluso si se trata de un intermediario establecido en la UE, pero en el caso de los que están establecidos fuera de la misma también es una herramienta para asegurar el cumplimiento

[73] D. J. B. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network, 2019, p. 147. Este autor ha bautizado esta tendencia como *"rep localization"* haciendo un paralelismo con la *"data localization"*.

[74] Freedom House, "Turkey", *Freedom of the Net 2020,* 2021. Disponible en: https://freedomhouse.org/country/turkey/freedom-net/2020

[75] Véase carta de la Autoriteit Persoonsgegevens de 10 de diciembre de 2020. Disponible en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf

[76] Si no se ha designado un representante legal específico, existe una extrema urgencia o éste no cumple con la orden, podrán remitirse a cualquier establecimiento del proveedor en la UE si es que lo tiene.

del Reglamento. La regulación de la designación de este representante se hace en una directiva independiente[77] que se aplicará a los proveedores de servicios que ofrezcan sus servicios en la UE y tengan (de nuevo) un vínculo sustancial con alguno de los Estados miembros (art. 1 y 2).

**36.** Algo muy similar ocurre con el art. 16 de la propuesta de Reglamento TERREG, que establece que los prestadores de servicios de alojamiento de datos que no tengan un establecimiento en la UE, pero que ofrezcan servicios en la misma, designarán por escrito a una persona física o jurídica como representante legal en la UE a efectos de la recepción, el cumplimiento y la ejecución de las órdenes de retirada, los requerimientos, las solicitudes y las decisiones emitidos por las autoridades competentes con arreglo al Reglamento. El representante legal deberá residir o estar establecido en uno de los Estados miembros en los que el prestador de servicios de alojamiento de datos ofrezca los servicios. El prestador de servicios de alojamiento de datos encomendará al representante legal la recepción, el cumplimiento y la ejecución de las órdenes de retirada, los requerimientos, las solicitudes y las decisiones en nombre del prestador de servicios de alojamiento de datos correspondiente. Los prestadores de servicios de alojamiento de datos otorgarán a su representante legal los poderes y recursos necesarios para cooperar con las autoridades competentes y cumplir esas decisiones y órdenes. El representante legal designado puede ser considerado responsable del incumplimiento de las obligaciones fijadas en el Reglamento, sin perjuicio de la responsabilidad del prestador de servicios de alojamiento de datos y de las acciones legales que podrían iniciarse contra este.

**37.** Según el art. 11 de la DSA, los prestadores de servicios intermediarios que no tengan un establecimiento en la UE pero que ofrezcan servicios en la misma designarán a una persona física o jurídica como su representante legal en uno de los Estados miembros donde el prestador ofrezca sus servicios. Los prestadores de servicios intermediarios mandatarán a sus representantes legales, además o en lugar del prestador, como destinatarios de las comunicaciones enviadas por las autoridades de los Estados miembros, la Comisión y la Junta sobre todas las cuestiones necesarias para la recepción, el cumplimiento y la ejecución de las decisiones adoptadas en relación con el Reglamento. Los prestadores de servicios intermediarios otorgarán a su representante legal las facultades y los recursos necesarios para cooperar con las autoridades de los Estados miembros, la Comisión y la Junta y cumplir esas decisiones. Se podrán exigir responsabilidades al representante legal designado por el incumplimiento de las obligaciones estipuladas en el Reglamento, sin perjuicio de la responsabilidad del prestador de servicios intermediarios y de las acciones legales que puedan iniciarse contra este.

**38.** En la propuesta de IAI, también se establece en su art. 25 que antes de comercializar sus sistemas en la UE, cuando no se pueda identificar a un importador, los proveedores establecidos fuera de la UE tendrán que designar, mediante un mandato escrito, a un representante autorizado que se encuentre en el territorio de la UE. Éste tendrá que cooperar con las autoridades nacionales competentes en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo y proporcionar a una autoridad nacional competente toda la información y la documentación necesarias para demostrar que un sistema de IA de alto riesgo cumple los requisitos establecidos en el Reglamento.

**39.** En realidad, una vez que las compañías establecen un representante en un Estado miembro para cumplir el RGPD, el exigirles un representante para cumplir el resto de la legislación es menos costoso, porque pueden designar al mismo representante para dar cumplimiento a todas estas normas, aunque sus competencias sean diferentes. Además, al final se trata de establecer un solo representante para los 27 Estados miembros, así que el coste no parece en general desproporcionado porque se trata de poder ofrecer servicios en un mercado del tamaño total de la UE, aunque evidentemente esto dependerá del tamaño de las empresas y los servicios que preste y si la UE es un mercado principal o secundario en sus operaciones.

[77] Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, COM/2018/226 final.

## 4. Sanciones por incumplimiento

**40.** El RGPD va acompañado de un régimen disuasorio de sanciones por su incumplimiento que busca que las empresas tengan un fuerte aliciente para cumplir con sus obligaciones. Así, su artículo 83.5 y 6 regula que las infracciones más graves se sancionarán con multas administrativas de 20 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Esto puede llevar a multas multimillonarias en el caso de las grandes empresas tecnológicas. Además, cabe señalar que el porcentaje no se aplica al volumen de negocio en la UE sino al global. Algunos expertos consideran que el riesgo de multas potenciales elevadas es una barrera importante para las pequeñas y medianas empresas, dado que su acceso a asesoramiento legal sofisticado sobre cuestiones legales complejas es limitado,[78] mientras que las multinacionales cuentan con grandes asesorías jurídicas.

**41**. No obstante, en la práctica, aunque ha habido multas elevadas, éstas no se han acercado a dicho potencial. Así si tenemos en cuenta las multas impuestas hasta ahora,[79] la más elevada fue de 50 millones de euros a Google Inc. el 21 de enero de 2019 por Francia debido a una vulneración de los artículos 5, 6, 13 y 14 RGPD por carecer de una base legal para el procesamiento de datos personales.[80] La segunda multa en cuantía fue impuesta por Alemania el 1 de octubre de 2020 y ascendió a 35 millones de euros a H&M debido a una vulneración de los artículos 5 y 6 RGPD por carecer de un base legal para el procesamiento de datos personales.[81] La tercera fue impuesta por Italia a TIM (el operador de telecomunicaciones) el 15 de enero de 2020, ascendió a casi 28 millones de euros y fue motivada por una vulneración de los artículos 5, 6, 17, 21 y 32 RGPD por carecer de una base legal para el procesamiento de datos personales. La Agencia luxemburguesa parece estar considerando una posible multa a Amazon de 425 millones de euros, lo que representaría aproximadamente el 2% de los ingresos netos reportados por Amazon de 21,3 mil millones de dólares en 2020, y el 0,1% de sus 386 mil millones de dólares en ventas, pero esto es sólo una propuesta que se está discutiendo en el mecanismo de coordinación del CEPD.[82]

**42**. En España, la multa más elevada fue impuesta a Vodafone España el 11 de marzo de 2021, de 8 millones de euros y se debió a una vulneración de los derechos de los interesados y, en particular, de los artículos 21, 24, 28 y 44 RGPD, el 21 de la a Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, el artículo 48 (1) b) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y el artículo 23 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de Derechos Digitales.[83]

**43.** Estas multas quedan por debajo del potencial del RGPD y también están por debajo de las más altas impuestas en Estados Unidos que no cuenta con una ley general de protección de datos, sino sectoriales o de determinados Estados. En Estados Unidos la multa más alta impuesta por la *Federal*

[78] D. J. B. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network, 2019, p. 146.

[79] A 8 de abril de 2021. Pueden seguirse las sanciones impuestas en los diferentes Estados de la UE en https://www.enforcementtracker.com/

[80] Véase *Délibération n°SAN-2019-001 du 21 janvier 2019 Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*. Disponible en : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/

[81] Véase M. Schemm "35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M", *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit,* 2020. Disponible en: https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren

[82] S. Schechner, « Amazon Faces Possible $425 Million EU Privacy Fine », *Wall Street Journal,* 10/06/2021 https://www.wsj.com/articles/amazon-faces-possible-425-million-eu-privacy-fine-11623332987

[83] Véase la Resolución de Procedimiento Sancionador de la Agencia europea de Protección de Datos de 11 de febrero de 2021, Procedimiento Nº: PS/00059/2020. Disponible en: https://www.aepd.es/es/documento/ps-00059-2020.pdf

*Trade Commission* (FTC) correspondió a Facebook en 2019 y ascendió a 5000 millones de dólares,[84] muy por encima de la impuesta a Equifax ese mismo año de 575 millones de dólares.[85]

**44.** A pesar de lo cuantioso de estas multas las empresas pueden obtener ventajas mucho mayores haciendo un uso ilícito de los datos y, por tanto, pueden llegar a internalizarlas como un coste más, como el precio por hacer determinados negocios, diluyéndose así su carácter desincentivador por el análisis coste/beneficio. Incluso, modelos de negocio que podrían considerarse incompatibles con el RGPD siguen existiendo por falta de un control y aplicación efectiva de éste, como, por ejemplo, las empresas que se dedican a la colocación de anuncios a través de *real-time bidding* sin una base legítima para tratar datos de los interesados.[86]

**45**. El art. 23 dedicado a las multas administrativas de la propuesta del Reglamento de e-privacy replica el correspondiente del RGPD hasta tal punto que se dice expresamente que será de aplicación lo estipulado en el mismo respecto a las infracciones. Así, se fijan sanciones para las vulneraciones más graves de 20 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Esto es coherente con la idea de acercar el régimen de la protección de la privacidad de las comunicaciones electrónicas al de la protección de datos. Si bien la fijación de la cuantía de las sanciones para determinadas violaciones de la norma se dejaban a decisión de los Estados (artículos 23.4, 23.6 y 26). El Supervisor Europeo de Protección de Datos en su Opinión sobre la propuesta consideró muy positiva la armonización de regímenes, aunque en su opinión debería haberse completado y no haberse dejado la fijación de la cuantía de las sanciones por determinadas violaciones a los Estados.[87]

**46.** Sin embargo, la propuesta de Reglamento EPOC no fija la cuantía de las sanciones por su incumplimiento y, por tanto, no sigue esta tendencia. Su art. 13 establece que, sin perjuicio de lo dispuesto en las legislaciones nacionales que prevean la imposición de sanciones penales, los Estados miembros establecerán normas relativas a las sanciones pecuniarias aplicables en caso de incumplimiento de las obligaciones previstas en el Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Si bien el Reglamento sí que dispone que las sanciones pecuniarias deberán ser "eficaces, proporcionadas y disuasorias", algo bastante usual en las normas de este tipo.

**47**. La propuesta de Reglamento TERREG se situaría entre ambas opciones. Su art. 18 establece que los Estados miembros determinarán el régimen de sanciones aplicable a las infracciones de las obligaciones impuestas a los prestadores de servicios de alojamiento de datos en el Reglamento y tomarán todas las medidas necesarias para garantizar su aplicación. Dispone que las sanciones que se impongan serán eficaces, proporcionadas y disuasorias, y añade algunos elementos que deben tenerse en cuenta en la fijación de la cuantía como la naturaleza, la gravedad y la duración de la infracción o su carácter doloso o culposo. Pero, además, se cierra el artículo dedicado a las sanciones con una cláusula que establece que los Estados miembros garantizarán que el incumplimiento sistemático de determinadas obligaciones impuestas en el Reglamento se someta a sanciones económicas de hasta el 4% del volumen de negocio

[84] Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook", *Federal Trade Commission,* 24/7/2019. Disponible en: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[85] Federal Trade Commission, "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach", *Federal Trade Commission,* 22/7/2019. Disponible en: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

[86] Véase M. Veale y F. Z. Borgesius. "Adtech and Real-time Bidding Under European Data Protection Law." *SocArXiv.* 1/04/2021.. doi:10.31235/osf.io/wg8fq y para una crítica más amplia véase S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile books, 2019.

[87] Véase European Data Protection Supervisor, *Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation),* p. 35. Disponible en: https://edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf

mundial del prestador de servicios de alojamiento de datos en el último ejercicio. Esto denota una clara influencia del RGPD, si bien se abandona la mención a los 20 millones de euros. En lo referente a las normas que tienen que ver con la moderación de contenidos y, por tanto, pueden afectar a la libertad de expresión es importante no crear un incentivo tan fuerte que lleve al bloqueo sistemático de contenido legal por miedo a las sanciones.

**48.** En la propuesta de DSA, su art. 42 dispone que los Estados miembros establecerán el régimen de sanciones aplicable en caso de incumplimiento del Reglamento por los prestadores de servicios intermediarios bajo su jurisdicción y se asegurarán de que el máximo importe de las mismas no exceda del 6% de la renta o facturación anual del prestador de servicios intermediarios afectado. Las sanciones por proporcionar información incorrecta, incompleta o engañosa, por no responder o rectificar información incorrecta, incompleta o engañosa o por no someterse a una inspección sobre el terreno no excederán del 1% de la renta o facturación anual del prestador afectado. A esto se añade que los Estados miembros se asegurarán de que el máximo importe de una multa coercitiva no exceda del 5 % de la facturación media diaria del prestador de servicios intermediarios afectado en el ejercicio fiscal anterior por día, calculado a partir de la fecha especificada en la decisión de que se trate. Las multas que corresponde imponer a la Comisión Europea a las plataformas en línea de muy gran tamaño tienen los mismos límites (art. 59 y 60). De nuevo, podemos ver la influencia del RGPD, si bien en la DSA se es más ambicioso al fijar un límite superior del 6% y además incluir multas coercitivas diarias.

**49.** La propuesta de DMA va todavía más lejos al establecer que la Comisión podrá en determinados casos imponer a un guardián de acceso multas que no excedan del 10% de su volumen de negocios total en el ejercicio financiero anterior y multas coercitivas que no excedan del 5% del promedio diario del volumen de negocios del ejercicio financiero anterior por día (arts. 26 y 27). Estos 5% y 10% traen su causa en que son los límites máximos de las multas por incumplimiento del Derecho de la competencia que impone la Comisión Europea.[88] Cabe señalar que las mayores multas impuestas por ésta debido a la vulneración del Derecho a la competencia han sido a Google por abuso de posición dominante, en 2017 en la comparación de servicios de venta de 4 342 865 000 euros (1 921 666 000 solidariamente con Alphabet)[89], en 2018 en el marco del sistema operativo Android y las aplicaciones móviles de 2 424 495 000 (conjuntamente con Alphabet)[90], y en 2019 en el marco de la colocación de anuncios de 1 494 459 000 euros (de los cuales 130 135 475 con Alphabet) [91]. No obstante, a pesar de la alta cuantía de estas multas en términos absolutos siguen siendo una fracción mínima de los beneficios de dichas empresas.

**50**. La propuesta de AIA establece, según su art. 71, para las infracciones más graves multas administrativas de hasta 30 millones de euros o, si el infractor es una empresa, de hasta el 6% del volumen de negocio total anual mundial del ejercicio financiero anterior.

[88] Véase art. 23 del Reglamento (CE) n° 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado, *DOUE* L 1, 4 de enero de 2003, p. 1.

[89] Véase Summary of Commission decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39740 — Google Search (Shopping)) (notified under document number C(2017) 4444), *DOUE* C 9, 12 de nero de 2018, p. 11, que fue objeto del Recurso interpuesto ante el Tribunal General de la UE el 11 de septiembre de 2017, Google y Alphabet c. Comisión, as. T-612/17.

[90] Véase Summary of Commission Decision of 18 July 2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.40099 — Google Android, 2019/C 402/08, C/2018/4761, *DOUE* C 402, 28 de noviembre de 2019, p. 19, que ha sido objeto del Recurso interpuesto ante el Tribunal General de la UE el 9 de octubre de 2018 — Google y Alphabet c. Comisión, as. T-604/18.

[91] Véase Summary of Commission Decision of 20 March 2019 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case T.40411 – Google Search (AdSense)) (notified under document number C(2019) 2173), 2020/C 369/04, C/2019/2173, *DOUE* C 369, 3 de noviembre de 2020, p. 6, que ha sido objeto del Recurso ante el Tribunal General de la Unión Europea interpuesto el 4 de junio de 2019, Google y Alphabet c. Comisión, as. T-334/19.

## 5. Autoridad de control

**51.** Una de las razones del éxito de las normas europeas de protección de datos debería ser la arquitectura institucional creada para ello. El RGPD dispone que cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (bautizadas como autoridades de control) supervisar la aplicación del mismo.

**52**. La figura de la autoridad de control (también conocidas como Autoridades de Protección de Datos o APD) no es una novedad del RGPD, sino que ya aparecía en su predecesora la Directiva de protección de datos personales de 1995.[92] De hecho, varios Estados europeos ya tenían autoridades de control antes, la Agencia Española de Protección de Datos se creó en 1992 y comenzó a funcionar en 1994.

**53.** La primera norma a nivel europeo de protección de datos personales, de hecho, no procedía de la UE sino del Consejo de Europa y fue el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, que tiene un Protocolo adicional sobre las autoridades supervisoras y los flujos transfronterizos de datos de 2004. Este último ha sido ratificado por 56 Estados, parte de ellos no europeos como Argentina, Cabo Verde, Mauricio, México, Marruecos, Senegal, Túnez y Uruguay.[93]

**54.** Lo que hace el RGPD frente a la Directiva de 1995 es detallar más las características de las autoridades de control y reforzar sus capacidades. Se fijan los requisitos que estas autoridades deben cumplir respecto a su independencia (art. 52), las condiciones generales aplicables a sus miembros (art. 53), las normas relativas a su establecimiento (art. 54), sus competencias (art. 55 y 56), funciones (art. 57) y poderes (art. 58).

**55.** La Comisión Europea cuando evalúa si un Estado ofrece un nivel de protección esencialmente equivalente al europeo, como ya se ha explicado no sólo se fija en la legislación, sino en que esos países cuenten con una autoridad de control independiente y efectiva. En ese sentido, Japón tuvo que crear su autoridad de control en 2016 para poder aspirar a una decisión de adecuación y Corea del Sur reformó su sistema de control centralizando las competencias que se repartían entre varios órganos en una autoridad de control única e independiente en 2020 con el mismo objetivo.

**56.** Las autoridades europeas de control se coordinan a través del Comité Europeo de Protección de Datos (CEPD) que es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la UE. Está compuesto por el director de las autoridades nacionales de protección de datos de todos los Estados miembros de la UE y de los Estados de la Asociación Europea de Libre Cambio (porque el RGPD se aplica en todo el Espacio Económico Europeo) y el Supervisor Europeo de Protección de Datos (SEPD). Tiene un papel muy importante porque es el que elabora las directrices sobre cómo deben interpretarse los artículos y conceptos del RGPD, además de otras muchas competencias (art. 70 RGPD). Vino a sustituir al Grupo de Trabajo del artículo 29 que existía con la Directiva de 1995, pero con competencias reforzadas.

**57.** Teniendo todo esto en cuenta, no es de extrañar que en su propuesta de Reglamento *e-privacy,* la Comisión Europea estableciera que las autoridades de control independientes encargadas de supervisar la aplicación del RGPD también serían responsables de supervisar la aplicación de este Reglamento (art. 18), dando competencias similares también al Comité Europeo de Protección de Datos (art. 19). Esto fue considerado como una clara mejora de la situación actual que permite que la supervisión quede en manos de otras autoridades (como los reguladores de telecomunicaciones) por las organizaciones de

[92] 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, *DOUE* L 281 de 23 de noviembre de 1995, p. 31.

[93] A 11 de junio de 2021.

protección de los derechos de los usuarios de Internet que entendían que ayudaría a una aplicación más coherente de la normativa.[94] Sin embargo, el Consejo de la UE en su orientación general de cara a la negociación con el Parlamento Europeo en el trílogo ha propuesto modificar el art. 18 y permitir que sean los Estados los que elijan a la autoridad que se encargue de la supervisión del Reglamento que podría ser diferente de las APD, aunque tendrían que coordinarse con ellas y ser también independientes.[95] Esto tendrá que acordarse entre el Parlamento y el Consejo.

**58.** Es necesario dotar a las APD de mayores recursos financieros, personales y técnicos. En una encuesta a 30 APD europeas sólo 9 se mostraban satisfechas con los recursos con los que contaban[96] y muchas han dado la voz de alarma por considerar que están muy por debajo de lo que sería apropiado.[97] La mayoría de las APD europeas necesitarían un aumento en su presupuesto del 30-50%, y hay algunos ejemplos extremos en los que esta necesidad se acerca incluso al 100%.[98] La Comisión considera la falta de recursos un problema sistemático y muy serio,[99] ha subrayado la obligación de los Estados miembros de asignar suficientes recursos a las APD y les ha instado a aumentarlos en múltiples ocasiones.[100] La sociedad civil también se ha expresado en el mismo sentido.[101]

**59.** Por su parte, la aplicación de los Reglamentos TERREG y EPOC será directamente supervisada por las autoridades judiciales de los países por lo que no era necesario crear una autoridad independiente especializada.

**60.** Respecto a la propuesta de DSA, los Estados miembros designarán una o varias autoridades competentes responsables de la aplicación y ejecución del Reglamento y en particular a una de ellas como su coordinador de servicios digitales. Esta nueva figura del "coordinador de servicios digitales" será responsable en todas las materias relacionadas con la aplicación y ejecución del Reglamento en ese Estado miembro, a menos que el Estado miembro de que se trate haya asignado determinadas funciones o sectores específicos a otras autoridades competentes. En todo caso, el coordinador de servicios digitales será responsable de garantizar la coordinación en el ámbito nacional y de contribuir a la aplicación y ejecución efectiva y coherente del Reglamento en toda la UE (art. 38). El Reglamento establece los requisitos de estos coordinadores que deberán ser totalmente independientes y un buen número de competencias. Esta figura recuerda *mutatis mutandis* a las APD. De hecho, los coordinadores de servicios digitales también se coordinarán a través de una Junta Europea de Servicios Digitales (JESD) que podría asimilarse, salvando las distancias, al CEPD.[102]

---

[94] EDRI, *EDRi's position on the proposal of an e-Privacy Regulation*, 2017, p. 11. Disponible: https://edri.org/files/epd-revision/ePR_EDRi_position_20170309.pdf

[95] General Secretariat of the Council, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP, doc. 6087/21. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=ES

[96] European Data Protection Board, *Individual replies from the data protection supervisory authorities*, 2020. Disponible en: https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[97] Politico EU, "EU privacy regulators voice alarm over GDPR, documents show", 2020. Disponible en: https://pro.politico.eu/news/eu-privacy-regulators-alarm-problems-documents

[98] Comité Europeo de Protección de Datos, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, 2019, p. 7. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

99 Comisión Europea, *Draft General budget of the European Union for the financial year 2021, Volume 9*, 2020, p. 2. Disponible en: https://eur-lex.europa.eu/budget/data/DB/2021/en/SEC09.pdf

[100] Comunicación de la Comisión al Parlamento Europeo y al Consejo La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos, COM/2020/264 final.

[101] Access Now, *Two years under the EU GDPR an implementation progress report,* 2020. Disponible en: https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

[102] El paralelismo es incluso más claro cuando se utilizan los términos en inglés de *European Board for Digital Services* y *European Data Protection Board*.

**61.** La Junta adoptará dictámenes, solicitudes y recomendaciones dirigidos a los coordinadores de servicios digitales u otras autoridades competentes nacionales. Aunque no sean legalmente vinculantes, la decisión de desviarse de ellos debe explicarse debidamente y puede ser tenida en cuenta por la Comisión para evaluar el cumplimiento de la DSA. La Junta también colaborará en la preparación de unos modelos y códigos de conducta pertinentes y analizará las tendencias generales emergentes en el desarrollo de servicios digitales en la UE. Una diferencia interesante respecto a CEPD es que en este caso la Comisión propone ser ella la que presida la Junta mientras que en el CEPD las APD eligen a un presidente entre ellas. Esto permitirá a la Comisión un mayor control sobre este organismo.

**62.** Respecto a los supervisores nacionales surge la gran duda de quién se encargará de estas funciones, si organismos nuevos o ya existentes, lo más probable es que estas competencias sean asumidas por organismos ya existentes, pero no tiene que por qué ser necesariamente así. Francia, por ejemplo, ha decidido crear un órgano que concentre un gran número de competencias, la *Autorité de régulation de la communication audiovisuelle et numérique* (ARCOM), que surge de la fusión del *Conseil supérieur de l'audiovisuel* (CSA) y de la *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (Hadopi).[103] Este órgano controlaría la aplicación de la DSA, e incluso antes de la *Loi confortant le respect des principes de la République* en la que Francia ha introducido algunos de los contenidos de la DSA en lo que respecta a la moderación de contenidos y la *Loi relatif à la protection de l'accès du public aux œuvres culturelles à l'ère numérique.*

**63**. La propuesta de DSA también copia uno de las cuestiones más conflictivas del RGPD y es su idea de crear un supervisor de establecimiento que es el llamado a tener jurisdicción sobre los intermediarios cuyo establecimiento principal esté en su país. Como es usual que un intermediario de Internet oferte sus servicios en varios Estados miembros de la UE para racionalizar el trabajo de las autoridades de control respectivas el RGPD estableció el mecanismo de "ventanilla única" (*one-stop-shop*), que garantiza la cooperación entre las autoridades de protección de datos para el tratamiento transfronterizo. Si una empresa realiza el tratamiento de datos en distintos países, la autoridad competente (que será la autoridad principal en sus relaciones con otras autoridades implicadas en la UE) es la del país de la UE en el que tenga su establecimiento principal. Esta solución que en teoría es muy lógica se ha revelado como una mala idea.

**64.** En una resolución del Parlamento Europeo de 2021 sobre la ejecución del RGPD, éste subrayó que la ventanilla única es útil para proporcionar seguridad jurídica y reducir la carga administrativa tanto para las empresas como para los ciudadanos. Sin embargo, expresó gran preocupación por su funcionamiento en la práctica, en particular por lo que se refiere al papel de las autoridades irlandesa y luxemburguesa. Observó que estas autoridades de protección de datos son las encargadas de tramitar un gran número de asuntos, puesto que muchas empresas tecnológicas han registrado su sede en la UE en esos países. Expresó su especial preocupación por que la autoridad irlandesa archive la mayoría de los casos con un acuerdo en lugar de una sanción y por que los casos remitidos a Irlanda en 2018 ni siquiera hubieran alcanzado la fase de proyecto de decisión en 2021. El Parlamento pidió a estas autoridades que aceleraran las investigaciones en curso sobre los asuntos de mayor relevancia para mostrar a los ciudadanos de la UE que la protección de datos es un derecho protegido jurídicamente en la UE y señaló que el éxito del "mecanismo de ventanilla única" depende del tiempo y del esfuerzo que las autoridades de protección de datos puedan dedicar a la tramitación y la cooperación en casos transfronterizos individua-

[103] A pesar de que Reino Unido no forma ya parte de la UE, también sigue esta tendencia de creación de órganos administrativos de control. En su caso, se ha decidido que la *Office of Communications* (Ofcom), que era el regulador de contenidos audiovisuales, se encargue también de la tarea de controlar que los intermediarios de Internet cumplen las medidas para luchar contra los *online harms*. Véase HM Government*, Online Harms White Paper: Full Government Response to the consultation*, 2020. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

Véase también *Draft Online Safety Bill* 2021. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

les y que la falta de voluntad política y de recursos tiene consecuencias inmediatas en el funcionamiento de este mecanismo.[104]

**65**. A 31 de diciembre de 2020, Irlanda tenía la supervisión principal europea en 196 procedimientos. Sin embargo, la autoridad irlandesa había concluido solo cuatro procedimientos mediante una decisión final. En comparación, las autoridades supervisoras alemanas encargadas de la supervisión principal en 176 procedimientos, habían concluido 52 procedimientos con una decisión final en la misma fecha.[105] Desde mayo de 2018 hasta marzo de 2021, las APD impusieron 596 multas y sanciones por un total de 278.549.188 euros. Los datos sobre el uso de multas muestran una gran discrepancia entre los Estados miembros en la forma en que las APD utilizan sus poderes. La APD más activa (la española) había impuesto 223 multas desde mayo de 2018, mientras que las APD menos activas (las luxemburguesa y eslovena) aún no habían emitido ninguna multa.[106]

**66.** Muchas multinacionales tecnológicas tienen su sede principal en la UE en Irlanda por sus ventajas fiscales y el uso común del inglés. Esto hace que económicamente al país no le interese tener una agencia de protección de datos excesivamente estricta que los pueda incomodar y terminar con una importante fuente de ingresos y empleo. Así, la autoridad irlandesa se ha convertido en el cuello de botella que retrasa las medidas de supervisión y sanción en su caso a compañías como Google, Facebook, Microsoft o Apple.[107]

**67.** Esta cuestión ha llegado incluso al Tribunal de Justicia de la UE y el Abogado General Bobek aunque ha mostrado su apoyo al mecanismo de ventanilla única ha admitido que hay situaciones de inercia administrativa en las que una autoridad (por falta de experiencia y/o personal, o por cualquier otra razón) no adopta ninguna medida significativa para investigar posibles infracciones del RGPD y hacer cumplir sus reglas.[108]

**68.** Incluso el Supervisor Europeo de Protección de Datos, Wojciech Wiewiórowski, ha afirmado que la ventanilla única ha afectado al funcionamiento del RGPD y, como cuestión de principio, no está seguro de que éste sea el enfoque correcto. Dijo que los legisladores habían subestimado los problemas con la ventanilla única e indicó que prefería la propuesta inicial de RGPD de la Comisión Europea, que respaldaba un mecanismo de aplicación más centralizado, pero que el Consejo de la UE y el Parlamento Europeo modificaron en la versión final del texto. Wiewiórowski concluyó que, si bien en el momento de la adopción del RGPD, la ventanilla única fue aclamada como un modelo potencial a seguir, ahora debemos tener mucho cuidado de utilizarlo en otras normas.[109]

**69.** La Comisión no era ajena a estas cuestiones por lo que creó un mecanismo en la propuesta de DSA que le permite avocarse casos cuando se dé la inacción de un coordinador nacional. En particular, podrá actuar cuando se sospeche que ha habido una infracción por parte de una plataforma de gran tamaño y el coordinador de servicios digitales de establecimiento no haya adoptado ninguna medida de investiga-

[104] Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (2020/2717(RSP), párrafo 20.

[105] Datos extraidos de la Carta de U. Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, al Comité LIBE del Parlamento Europeo de 16 de marzo de 2021. Traducción al inglés no oficial disponible en: https://www.iccl.ie/wp-content/uploads/2021/03/Letter-BfDI-LIBE-on-Irish-DPC_EN.pdf

[106] Access Now, *Three years under the GDPR. An implementation progress report.* 2021, p. 2. Disponible en: https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf

[107] J. Ryan, *Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights Submission to the Joint Oireachtas Committee on Justice*, Irish Council of Civil Liberties, 2021, p. 3. Disponible en: https://www.iccl.ie/wp-content/uploads/2021/03/ICCL-submission-on-the-GDPR-to-the-Joint-Oireachtas-Committee-on-Justice-26-March-2021.pdf

[108] Conclusiones del Abogado General Sr. Michal Bobek de 13 de enero de 2021, Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit, as. C-645/19 ECLI:EU:C:2021:5, párrafo 114.

[109] V. Manancourt, « EU privacy law's chief architect calls for its overhaul », *Politico.eu* 25/05/2021. Disponible en: https://www.politico.eu/article/eu-privacy-laws-chief-architect-calls-for-its-overhaul/

ción o ejecución, a pesar de una solicitud en ese sentido de la Comisión. Es necesario que la aplicación de la futura norma no se pueda ver bloqueada como ha pasado con el RGPD y la autoridad irlandesa.

**70.** No obstante, algunos países como Francia preferirían que las autoridades de cada Estado pudieran sancionar a los intermediarios y están intentando modificar la propuesta en ese sentido, si bien desde la Comisión se considera que es mejor que las compañías tengan que lidiar con una sola autoridad en lugar de 27, porque lo contrario socavaría el mercado interior.[110]

**71.** Francia no quiere ser completamente dependiente de la capacidad de respuesta o de la voluntad de actuar rápidamente del regulador del país de origen. Si bien no quiere terminar con el principio de país de origen, sí que quiere matizarlo, por ejemplo, permitiendo a los reguladores locales imponer medidas provisionales en caso de emergencia, o exigiendo a los reguladores principales que compartan datos con otras autoridades, con la posibilidad de reasignar los casos "de mutuo acuerdo". Así una autoridad nacional, como la francesa, por ejemplo, preguntaría a su homóloga irlandesa si planea investigar una presunta infracción en Francia por parte de una gran plataforma como Google, Facebook o Twitter, y podría iniciar una investigación si no respondiera en tres semanas. Si la autoridad irlandesa decidiera abrir una investigación, tendría que permitir el acceso a toda la información del proceso e involucrar a la autoridad francesa en la decisión final. Francia también podría plantear una "objeción razonada" si no le gustara la decisión inicial de Irlanda y la Junta Europea de Servicios Digitales debería resolver los desacuerdos entre las autoridades nacionales si se cree que no se tomaron medidas o que el resultado de una investigación no fuera satisfactorio.[111]

**72**. En la propuesta de DMA, no se propone la creación de autoridades independientes de supervisión porque, al igual que ocurre con el Derecho de la competencia al que este Reglamento complementa, cuando un problema afecta al mercado interior en su conjunto no sólo a un Estado, como será el caso por definición de los guardianes de acceso, es la Comisión la que lleva a cabo la investigación y toma las medidas pertinentes.

**73.** Según el art. 59 de la AIA, cada Estado miembro establecerá o designará autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución del Reglamento. Las autoridades nacionales competentes se organizarán de manera que se preserve "la objetividad e imparcialidad de sus actividades y funciones". Cada Estado miembro designará una autoridad nacional de supervisión entre las autoridades nacionales competentes.[112] La autoridad nacional de supervisión actuará como autoridad notificante y como autoridad de vigilancia del mercado, salvo que un Estado miembro tenga razones organizativas o administrativas para designar más de una autoridad.

**74**. El art. 56 de la propuesta establece un Comité Europeo de Inteligencia Artificial (CEIA) integrado por representantes de los Estados miembros y la Comisión. De nuevo será presidido por la Comisión, como en la propuesta de DSA, a diferencia del CEPD. El Comité facilitará la aplicación sencilla, efectiva y armonizada de este Reglamento contribuyendo a la cooperación efectiva de las autoridades nacionales de supervisión y la Comisión, así como proporcionando asesoramiento y conocimientos especializados a esta última. Además, compilará y compartirá las mejores prácticas entre los Estados miembros.

---

[110] J. Espinoza y L. Abboud, "France pushes for big changes to proposed EU tech regulation", *Financial Times,* 15/2/2021. Disponible en: https://www.ft.com/content/5e41d0cf-a83c-4817-997e-a353858137ab

[111] L. Kayali, "France's plan to rein in Big Tech (and Ireland and Luxembourg)", *Politico.eu,* 27/05/2021. Disponible en: https://www.politico.eu/article/france-ireland-luxembourg-big-tech-regulation-apple-amazon-facebook-google-digital-services-act-digital-markets/

[112] Incluso entre los propios Estados miembros existen muchas dudas sobre cuáles serán estas autoridades y es un tema que puede conllevar bastante discusión. Véase intervención de M. Valle del Olmo, Coordinador de Área Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales de la Secretaría de Estado de Digitalización e Inteligencia Artificial en la "Jornada el Nuevo Reglamento de inteligencia artificial de la UE" organizada por OdiseIA, FIAL y SEDIA (24/4/21). Disponible en: https://www.youtube.com/watch?v=xil56RRg3Gc

**75.** Según Access Now, el mecanismo de ejecución propuesto carece de claridad. En su opinión, la creación de un nuevo comité y el nombramiento de autoridades de supervisión con responsabilidades y competencias que pueden solaparse con las del CEPD y las APD existentes podría causar confusión y, en el peor de los casos, socavar la autoridad del CEPD y las APD en asuntos que son fundamentales para sus competencias.[113]

***Tabla 1.*** *Impacto del RGPD en las propuestas normativas de regulación digital de la Comisión Europea*

| | **RGPD** | **e-Priv.** | **EPOC** | **TERREG** | **DSA** | **DMA** | **IAI** |
|---|---|---|---|---|---|---|---|
| Aplicación extraterritorial | SÍ | SÍ | SÍ | SÍ | SÍ | SÍ | SÍ |
| Necesidad de representante en la UE | SÍ | SÍ | SÍ | SÍ | SÍ | NO | SÍ |
| Multas de % como máximo del volumen de negocio anual global del ejercicio anterior | 4% | 4% | NO | 4% | 6% | 10% | 6% |
| Autoridad independiente de control | APD | APD | NO | NO | Coord. Serv. Dig. | Comi. | ¿? |
| Creación de comité europeo de coordinación | CEPD | CEPD | NO | NO | JESD | NO | CEIA |

Fuente: elaboración propia.

## III. Conclusiones

**76.** El RGPD ha tenido un fuerte impacto en el ámbito de la protección de datos tanto fuera como dentro de las fronteras de la UE. Pero también ha servido como inspiración para el resto de iniciativas regulatorias importantes de la Comisión Europea en el marco del Mercado Único Digital, sobre todo en lo relativo a la regulación de los intermediarios de Internet. Desde que la Comisión presentó la propuesta de RGPD hasta que se adoptó pasaron 4 años de duras negociaciones entre el Parlamento Europeo y el Consejo de la UE,[114] que sufrieron un intenso lobby. Así el resultado fue un compromiso muy trabajado.

**77**. Por eso no es de extrañar que una legislación que ha servido como modelo para las leyes de protección de datos haya sido también seguida por la Comisión Europea en otras propuestas normativas relevantes que siguen el impulso de constitucionalismo digital inaugurado por el RGPD.

**78.** Esta influencia puede verse claramente en las propuestas de Reglamento e-privacy, el Reglamento EPOC, el Reglamento TERREG, la DGA, la DSA, la DMA y la AIA, aunque en unos casos con mayor intensidad que en otros. En particular, en este artículo se han estudiado la mimesis en los mecanismos que buscan asegurar mejor el cumplimiento de estas normas, especialmente teniendo en cuenta que en muchas ocasiones sus destinatarios se encontrarán situados fuera del territorio de la UE. Así se ha podido ver la replicación del modelo del RGPD en lo referente a: su naturaleza de reglamento, la aplicación extraterritorial, la obligación de que algunas empresas localizadas fuera de la UE nombren a un representante dentro de la misma, la necesidad de autoridades independientes de control en cada Estado para vigilar su aplicación que se agrupan en un comité europeo y la posibilidad de imponer multas elevadas por su incumplimiento.

**79.** Algunos de estos elementos que resultaron controvertidos en el RGPD se han convertido en la norma por la ventaja que suponen a la hora de proteger a los europeos, como puede ser la aplicación extraterritorial o la necesidad de designar a un representante. En ese sentido, este último ejemplo al final una vez que se nombra un representante para cumplir con una de estas normas la carga ya no es tan alta respecto a las demás porque el representante podría ser el mismo para todas ella.

[113] Access Now, "EU takes minimal steps to regulate harmful AI systems, must go further to protect fundamental rights", 21/04/2021. Disponible en: https://www.accessnow.org/eu-minimal-steps-to-regulate-harmful-ai-systems/

[114] Hasta tal punto que las negociaciones fueron objeto de la película *Democracy: Im Rausch der Daten* de David Bernet.

**80.** Es necesario aprender de los problemas que la experiencia ha revelado respecto a la aplicación del RGPD, como es que es imperativo dotar de recursos suficientes a las autoridades encargadas de vigilar del cumplimiento de las normas, si se quiere asegurar su efectividad. Los retos que ha planteado el *one-stop-shop* del RGPD deberían conllevar la búsqueda de mecanismos para aminorarlos en propuestas como la de la DSA, en ese sentido las propuestas de Francia resultan interesantes y no fragmentan el principio de mercado único.

**81.** Por otra parte, es obvia una inflación en la creación de comités europeos de concertación que siguen la estela del CEPD, como son la Junta Europea de Servicios Digitales, el Comité Europeo de Inteligencia Artificial y el Comité Europeo de Innovación en materia de Datos. Habrá que asegurar una correcta coordinación entre los mismos y que sus competencias no se solapen, y la Comisión Europea debería plantearse si es necesario crear tantos comités a nivel europeo.

**82.** También se puede ver como la tendencia a crear la posibilidad de cuantiosas sanciones ligadas a un porcentaje del volumen de negocio total anual global de las empresas ha continuado e incluso pasado de un máximo del 4% al 6% o incluso 10%. Esto es por la naturaleza disuasoria de las mismas, pero se ha visto que en la práctica no suelen imponerse multas tan elevadas.

**83.** Es muy importante que las nuevas propuestas de la Comisión incorporen las lecciones aprendidas en los tres años desde que empezó a aplicarse el RGPD, para aprovechar aquellos mecanismos que sean útiles y mejorar aquellos que hayan presentado problemas. La UE está buscando a través de su regulación de las cuestiones digitales influir no sólo dentro de sus fronteras sino también fuera como un emprendedor normativo. Por lo que debe aplicar correctamente estos mecanismos y aprender de sus propios errores para seguir creando estándares globales en lo relativo a los intermediarios de Internet y el sector digital.