DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

7

INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

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

Dykinson, S.L.

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

INTELIGENCIA ARTIFICIAL
Y DERECHO DE DAÑOS:
CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

COLECCIÓN
DERECHO DIGITAL Y PROPIEDAD INTELECTUAL

INTELIGENCIA ARTIFICIAL Y DERECHO DE DAÑOS: CUESTIONES ACTUALES

Acorde al Reglamento (UE) 2024/1689

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

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

Dykinson, S.L.

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

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

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

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

ISBN electrónico: 978-84-1122-801-5

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

Índice

Inteligencia artificial generativa y daños por infracciones normativas del derecho de protección de datos personales. Un análisis a partir de la jurisprudencia reciente del TJUE sobre el artículo 82 RGPD

ANTONI RUBÍ PUIG [1]

Profesor agregado de derecho civil, Universitat Pompeu Fabra

[1] Este capítulo se ha preparado en el marco del proyecto PID2021-126354OB-I00/MICIN/AEI/10.13039/501100011033/FEDER, UE, sobre "Responsabilidad contractual y extracontractual de las plataformas en línea" financiado por el Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación y el Fondo Europeo de Desarrollo Regional.

1. INTRODUCCIÓN

Los últimos dos años han sido testigos de importantes desarrollos y mejoras en el campo de la inteligencia artificial generativa (en adelante, «IA generativa»), que han contribuido a su popularidad y a su utilización crecientes. Sistemas y servicios como ChatGPT, Dall-E, Bard, Stable Diffusion, Midjourney, Sora o Copilot permiten a sus usuarios impartir instrucciones (*prompts*) o emplear otros *inputs* para obtener resultados sintéticos en forma de textos, imágenes, videos o código fuente informático. También bots conversacionales, asistentes virtuales e instrumentos de búsqueda se basan en modelos de IA generativa para ofrecer respuestas más complejas y de mayor calidad en las interacciones con sus usuarios. La IA generativa ha revolucionado asimismo la traducción, análisis y resumen de información. Todas estas herramientas de IA generativa se están utilizando ya en sectores tan diversos como la educación, la atención de clientes, la creación de contenidos o el ejercicio de profesiones jurídicas; y es esperable que su uso crezca en los próximos años.

El funcionamiento de los modelos y sistemas de IA generativa depende de varios elementos, pero sobre todo del acceso y uso de grandes cantidades de datos, así como de la variedad y calidad de estos. Para que un modelo pueda proporcionar unos determinados resultados mínimamente valiosos ha de haber sido entrenado previamente con bases de datos muy grandes[2]. Previsiblemente, cuantos más datos se utilicen en su entrenamiento, mejor será la calidad del modelo y de los resultados esperables[3]. Aunque OpenAI se guarda de ofrecer información sobre este extremo, se estima que GPT-4, uno de los modelos más potentes que ha desarrollado, fue entrenado a partir de más de 13 millones de *tokens* provenientes de bases de datos públicas como RefinedWeb y CommonCrawl, que rastrean y almacenan información de más de 2.700 millones de páginas web. Estas mismas bases de datos u otras diferentes -por ejemplo, elaboradas internamente, a partir de datos sintéticos- pueden ser utilizadas, además de en tareas de entrenamiento, para mejorar o afinar un modelo, para desarrollar sistemas y servicios personalizados y para alinear estos con determinados objetivos de calidad. Dada la extraordinaria cantidad de datos utilizados en todas estas tareas de la cadena de valor de la

---

[2] Novelli, C., Casolari, F., Hacker, P., Spedicato, G., y Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *ArXiv, abs/2401.07348*. 1-36. pág.1.

[3] Ahora bien, a partir de determinado umbral, el valor añadido que tiene sumar más datos crece a una tasa decreciente. En este sentido, véase Carrière-Swallow,Y., y Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective. *IMF Departmental Papers* 19 (16), 2019. 1-46. Además, algunos autores critican también que necesariamente cuantos más datos traten y más grandes sean los modelos de IA, mejores serán. En este sentido, véase Varoquaux, G., Luccioni, A.S., y Whittaker, M. (2024). Hype, Sustainability, and the Price of the Bigger-is-Better Paradigm in AI. (https://doi.org/10.48550/arXiv.2409.14160).

IA generativa, es altamente probable, sino seguro, que muchos de ellos serán datos de carácter personal y que, por tanto, su uso y, en general, el funcionamiento de modelos y sistemas comportarán actos de tratamiento de datos personales.

En estos momentos de emergencia de la tecnología, persisten muchas dudas acerca de las implicaciones jurídicas que despliega la IA generativa en el derecho de protección de datos. En la Unión Europea, son muchas las cuestiones abiertas acerca de la aplicación del Reglamento General de Protección de Datos («RGPD»[4]) a la IA generativa[5]. Las dudas no son exclusivas de este sector jurídico y se proyectan también en ámbitos tales como la responsabilidad civil y la protección de los derechos de propiedad intelectual[6].

En el ámbito de la protección de datos personales, se han entablado recientemente varios procedimientos contra algunos de los proveedores de servicios de IA generativa más conocidos en los cuales se habrán de discutir cómo estos han de cumplir con las exigencias establecidas en el RGPD y otras normas[7]. También algunas agencias de protección de datos o autoridades de supervisión han elaborado ya guías y otros documentos acerca de las interacciones entre IA generativa y protección de datos personales[8]. En la literatura

---

[4] 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) (OJ L 119, 4.5.2016, pgs. 1-88) (en adelante, RGPD).

[5] Para una visión panorámica, véanse Marcos, H., y Pullin, M. (Octubre 2023). Large Language Models and EU Data Protection: Mapping (Some) of the Problems. *The Digital Constitutionalist*. https://digi-con.org/large-language-models-and-eu-data-protection-mapping-some-of-the-problems; Necati Pehlivan, C. (19 de septiembre de 2024). Inteligencia artificial y protección de datos. *Almacén de Derecho*. https://almacendederecho.org/inteligencia-artificial-y-proteccion-de-datos; y Nunez Duffourc, M., Gerke, S., y Kollnig, K. (2024). Privacy of Personal Data In The Generative AI Data Lifecycle. *New York University Journal of Intellectual Property And Entertainment Law*. Vol. 13, n. 2. 219-268.

[6] Véanse, entre otros, Lee, K., Cooper, F., y Grimmelmann, J. (2024). Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain. *Journal of the Copyright Society*, 2024. 1-128 (en prensa) (disponible a http://dx.doi.org/10.2139/ssrn.4523551); y Kretschmer, M., Margoni, T. y Oruç, P. (2024). Copyright Law and the Lifecycle of Machine Learning Models. *IIC*. vol. 55. 110-138.

[7] Para un resumen de diferentes procedimientos en marcha, véase Zanfir-Fortuna, G. (12 de septiembre de 2023). How Data Protection Authorities are De Facto Regulating Generative AI. *Future of Privacy Forum*. https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/. Véanse también, entre otros, Chiara, P.G. (2023). Italy: Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing. *European Data Protection Law Review*.Vol. 9. 68-72; y NYOB (6 de junio de 2024). noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI. https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai.

[8] European Data Protection Supervisor (3 de junio de 2024). Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems. https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf. Véanse, en relación con agencias nacionales de protección de datos,

académica, también se discuten las implicaciones para el derecho a la protección de los datos personales de los modelos y sistemas de IA generativa[9]. A la espera de cómo vaya concretándose este entendimiento y, en particular, en el caso europeo, de cómo los desarrolladores y operadores de modelos y sistemas de IA generativa hayan de cumplir con los requisitos establecidos en el RGPD, es asumible que en su desarrollo y funcionamiento se habrán cometido ya o se podrán cometer varias infracciones de esta normativa y causar daños con ello.

El objeto de este trabajo es identificar y discutir una serie de cuestiones que pueden llegar a suscitarse en relación con la reparación de los daños y perjuicios derivados de infracciones de la normativa de protección de datos cometidas en el ámbito de la IA generativa. Este trabajo no pretende ofrecer un tratamiento completo de este tema y, principalmente, por diversas limitaciones que lo impiden.

En primer lugar, no es posible ofrecer una discusión completa de la reparación de daños por infracciones de la normativa protectora del derecho a los datos personales en el campo de la IA generativa, pues, como se verá, el cumplimiento de la normativa dependerá de cómo funcione efectivamente cada modelo o sistema en cuestión. Si bien diferentes modelos y sistemas de IA generativa pueden compartir unos ciertos rasgos comunes, en la práctica operarán de modo diferente y contarán con diseños muy diversos, algunos más respetuosos que otros en la protección de los datos personales. Por ello, si sus desarrolladores y operadores han sido escrupulosos en el cumplimiento del RGPD o han adoptado unas cautelas superiores, que descarten la ilicitud del tratamiento, no deberán responder por los daños que causen y serán los afectados quienes hayan de pechar con ellos.

En segundo lugar, en función de cómo agencias de protección de datos y tribunales acaben entendiendo algunos de los problemas de aplicación de la normativa de protección de datos al funcionamiento de la IA generativa (en

---

los documentos siguientes: AEPD (febrero de 2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf; CNIL, "Les fiches pratiques sur l'IA", 2024 (https://www.cnil.fr/fr/les-fiches-pratiques-ia); y Garante per la Protezione dei Dati Personali (septiembre de 2023). Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale. https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+ la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0.

Véanse también las orientaciones ofrecidas por la confederación de asociaciones de delegados de protección de datos: Confederation of European Data Protection Organisations (16 de octubre de 2023). Generative AI: The Data Protection Implications. *CEDPO AI Working Group*. https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf.

[9] Véanse, entre otros, Ruschemeier, H. (2024). Generative AI and Data Protection. Calo, R., Ebers, M., Poncibò, C., y Zou, M. (2024). *Handbook on Generative AI and the Law*, Cambridge University Press (en prensa) (disponible en SSRN: https://ssrn.com/abstract=4814999).

particular, de la base de licitud para las tareas de entrenamiento de modelo), es probable que muchos de los daños esperables no sean tales o no sean indemnizables. Si, finalmente, se llega a la conclusión de que los tratamientos de datos personales y, en particular, de datos de categorías especiales, implicados en las tareas de entrenamiento de bases de datos cuentan con una base de licitud suficiente, desaparecería uno de los requisitos exigidos por el artículo 82 RGPD para fundar una pretensión indemnizatoria: no habría ya infracción normativa y, por ello, el daño si hubiera sido efectivamente sufrido por un individuo debería ser asumido por este. El legislador europeo no ha querido reducir la incertidumbre en este ámbito, como sí ha hecho en el caso de los derechos de autor mediante algunas normas del Reglamento de Inteligencia Artificial (en adelante, «RIA») [10]; y, por lo tanto, hay una deferencia hacia la elaboración descentralizada del derecho de protección de datos en este ámbito y la identificación progresiva de soluciones a los diferentes problemas planteados.

En tercer lugar, la IA generativa constituye un sector dinámico, con altos niveles de innovación. Muchas de estas innovaciones se dirigen a reducir los riesgos de la IA generativa y, en particular, a los riesgos en la intimidad y el derecho a la protección de los datos personales. Por ello, es probable que se reduzcan las situaciones en las cuales se terminen causando daños y perjuicios derivados de infracciones de la normativa sobre protección de datos personales. En este sentido, en los últimos años muchos investigadores implicados en lo que se conoce como *machine unlearning* proponen y elaboran mecanismos para reducir los impactos que la IA generativa puede tener en los derechos de protección de datos [11].

Por último, el trabajo no persigue un examen exhaustivo de la aplicación del artículo 82 RGPD a los daños y perjuicios ocasionados por tratamientos infractores de la normativa sobre protección de datos personales en la cadena de valor de la IA generativa, sino solamente destacar algunos aspectos que puedan

---

[10] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DO L, 2024/1689, 12.7.2024 (en adelante, «RIA»).

[11] Véanse, entre otros, Brown, H., Lee, K., Mireshghallah, F., Shokri, R., y Tramèr, F. (2022). What Does It Mean for a Language Model to Preserve Privacy?. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 2280-92. https://doi.org/10.1145/3531146.3534642; Hine, E., Novelli, C., Taddeo, M., y Floridi, L. (2023). Supporting Trustworthy AI Through Machine Unlearning. *SSRN Scholarly Paper*. https://doi.org/10.2139/ssrn.4643518; y Achille, A., Kearns, M., Klingenberg, C., y Soatto, S.0. (2023). AI model disgorgement: Methods and choices. *Proceedings of the National Academy of Sciences of the United States of America, 121 (https://doi.org/10.48550/arXiv.2304.03545).*

llegar a cobrar protagonismo en la litigación que surja en los próximos años. El trabajo no tiene, pues, una pretensión analítica y, en buena medida, se limita a identificar y describir brevemente las cuestiones jurídicas y problemas principales que permearán potenciales reclamaciones de daños y perjuicios al derecho de protección de datos personales en el campo de la IA generativa.

El trabajo se estructura del modo siguiente. Después de describir cómo funciona la IA generativa, identificar diferentes tratamientos de datos personales y su régimen jurídico básico bajo el RGPD, se presenta un conjunto de cuestiones que planteará la reparación de los daños en este ámbito de conformidad con el artículo 82 RGPD y la jurisprudencia del TJUE que lo ha interpretado. Estas cuestiones se refieren a los aspectos siguientes: la probabilidad de que los daños indemnizables lo sean por importes bajos o de bagatela; la indemnizabilidad del daño derivado del temor que datos personales puedan llegar a utilizarse maliciosamente; la causación de daños en supuestos de brechas de seguridad en el ámbito de la IA generativa; la compatibilidad de la pretensión prevista en el artículo 82 RGPD con otros fundamentos indemnizatorios; y los supuestos de pluralidad de sujetos responsables en los casos de múltiples participantes en la cadena de valor de la IA generativa. Finalmente, el trabajo presente unas breves conclusiones.

2. FUNCIONAMIENTO DE LA IA GENERATIVA E IMPLICACIONES PARA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

2.1. Concepto

La IA generativa es una modalidad de inteligencia artificial que permite la producción de diferentes resultados en forma de textos, imágenes, sonidos, vídeos, código fuente informático, modelos 3D u otros datos, a partir, en general, de la entrada de un texto u otro *input*. Así, por ejemplo, algunos sistemas, como los derivados de GPT-4, pueden ser multimodales y aceptar informaciones de entrada diferentes, como, por ejemplo, textos e imágenes.

El Reglamento de Inteligencia Artificial no se refiere expresamente a la IA generativa, pero sí incluye una serie de normas aplicables a los modelos de IA de uso general (*General Purpose Artificial Intelligence Model* (GPAIM)), que fueron adoptadas durante el proceso legislativo como reacción a la popularización de ChatGPT y otros sistemas. Según el artículo 3.63 RIA un «modelo de IA de uso general» es «*un modelo de IA, también uno entrenado con un gran*

volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado».

En efecto, muchos modelos de IA generativa –y en particular, los más avanzados– que se basan en aprendizaje automatizado o *machine learning* constituirán GPAIMs. La razón principal es que estos representan modelos de lenguaje extenso (MLE) (*Large Language Models* (LLM))[12], consistentes en redes neuronales artificiales que a partir de la detección de relaciones estadísticas entre los contenidos utilizados para entrenarlos pueden llevar a cabo, entre otras, tareas de generación de textos, procesamiento y clasificación de textos y otros contenidos. Por ello, algunas normas del RIA destinadas a los GPAIMs se aplicarán a los modelos y sistemas de IA generativa. La noción de uso general o finalidad general entra en conflicto con uno de los principios rectores del RGPD: el principio de limitación de la finalidad (arts. 5.1.b) y 6.4 RGPD). No es esta la única tensión, como se verá, entre las características de la IA generativa y el armazón y espíritu que permean el sistema europeo de protección de datos de carácter personal.

2.2. Tipología

Encontramos dos grandes tipos de sistemas de IA, basados en modelos de uso general: por un lado, los denominados clasificatorios, discriminatorios o predictivos y, por otro lado, los generativos. Los primeros sirven para tareas de clasificación mediante la atribución de un valor a partir de una información de entrada. Por ejemplo, plataformas de contenidos como YouTube utilizan modelos discriminatorios para identificar si un determinado vídeo que quiere subir un usuario es ilícito o no. O los sistemas de asignación de un *scoring* crediticio que utilizan los bancos son también clasificatorios[13]. En los sistemas clasificatorios, los valores atribuidos por el sistema son limitados: si no son binarios, habrá un número limitado de valores que podrán asignarse. En cambio, en los sistemas de IA generativos, la respuesta no está determinada por un

---

[12] También, en ocasiones, estos modelos de uso general se conocen como modelos fundacionales. La terminología fue desarrollada por un grupo de investigadores de la Universidad de Stanford. Véase Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., y Liang, P. (2023). Foundation Models and Fair Use. *Stanford Law and Economics Olin Working Paper* No. 584. https://ssrn.com/abstract=4404340.

[13] Véase STJUE de 7 de diciembre de 2023, asunto C-634/21, *OQ c. Land Hessen y SCHUFA Holding AG.* ECLI:EU:C:2023:957. Para un análisis del caso, véase Arroyo i Amayuelas, E. (2024). El scoring de Schufa. *InDret* 3.2024. 134-160.

número limitado de valores y, por tanto, no se puede predecir correctamente el resultado que ofrecerá el sistema. Esto es, a partir de un mismo *prompt*, entrada o instrucción, se pueden producir generaciones distintas, como textos o imágenes diversas que sólo se parecerían conceptualmente. La mejora de los sistemas generativos se debe sobre todo a los avances recientes en dos técnicas o arquitecturas que permiten optimizar los resultados esperables de los modelos subyacentes a partir de una descripción textual: los transformadores y la difusión[14].

2.3. Cadena de valor

2.3.1. General

El objeto de este apartado es presentar brevemente algunos aspectos relacionados con el funcionamiento de la IA generativa y destacar, sin ánimo de exhaustividad, algunas implicaciones para el derecho de la protección de datos[15]. Por ello, presentamos brevemente los diferentes elementos en el ciclo de vida o cadena de valor de la IA generativa, para mostrar que en su desarrollo y funcionamiento se llevan a cabo diferentes tratamientos de datos personales. Ello se debe en buena medida a que el RGPD parte de un concepto muy amplio de tratamiento de datos personales[16]. Con arreglo al artículo 4.2 RGPD, "tratamiento de datos personales" es *«cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso,*

---

[14] Por ejemplo, el modelo de ChatGPT usa técnicas de transformadores y de aquí su nombre (*Chat Generative Pre-trained Transformer*). Los modelos para generar imágenes sintéticas emplean técnicas de difusión. Véase Guadamuz, A. (2024). A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs. *GRUR International, 73*(2), 111-127. En especial, pág. 114.

[15] Para un análisis más detallado de la cadena de valor desde la perspectiva de los derechos de propiedad intelectual, véanse Lee, K., Cooper, F., y Grimmelmann, J. (2024). *Op. cit.*; y Guadamuz, A. (2024). *Op. cit.*. En el ámbito de la protección de datos personales, véase Mühlhoff, R., y Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology, 16*(1), 261-292. https://doi.org/10.1080/17579961.2024.2313794.

[16] Para Davara Rodríguez, M.A. (2021). Tratamiento (Comentario al Artículo4.2 RGPD). Troncoso Reigada A. (Dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. Tomo I, Thomson Reuters -Civitas. 591-628, pág. 592, *«tratamiento de un dato de carácter personal es hacer cualquier cosa con el mismo»*. Véase, también, STJUE de 24 febrero 2022, asunto C-175/20, *SS SIA c. Valsts ieņēmumu dienests*. ECLI:EU:C:2022:124, Apdo. 35.

cotejo o interconexión, limitación, supresión o destrucción». Se trata de un concepto claramente extenso, que comporta que la normativa prevista en el RGPD se aplique a casi cualquier tipo de uso de datos personales.

En consecuencia, las actividades relacionadas con la creación de bases de datos para el entrenamiento de modelos de IA generativa, el propio entrenamiento, el uso de un sistema de IA generativa y la producción de resultados comportarán las más de las veces tratamientos de datos personales, que habrán de cumplir con los requisitos legales establecidos en el RGPD y, en particular, con los principios generales recogidos en el artículo 5 RGPD.

Las características principales que pueden predicarse de los sistemas de IA generativa (tamaño, generalidad y opacidad) entran en clara contradicción con las líneas estructurales principales del sistema de protección del derecho de protección de datos personales establecido en el RGPD (minimización, limitación de los fines, transparencia). En consecuencia, es esperable que, salvo una intervención legislativa, en estos momentos acomodar la IA generativa al RGPD resulte ilusorio y el riesgo de infracción normativa no pueda eliminarse incluso para aquellos desarrolladores más cautelosos y que hagan esfuerzos mayores para alinear sus actividades con las obligaciones establecidas en el Reglamento.

2.3.2. Bases de datos

La cadena de valor de la IA generativa se inicia con la creación de bases de datos que luego se utilizarán para entrenar los modelos y, en su caso, para ajustarlos, corregirlos y verificar su funcionamiento óptimo. Las bases de datos utilizadas pueden ser de muchos tipos, pero, en general, suelen contener ingentes cantidades procedentes de diferentes tipos de fuentes y en formatos diferentes. Como se ha señalado, bases de datos como RefinedWeb y CommonCrawl almacenan información procedente de millones de páginas web, obtenida mediante técnicas de *scraping*. Otras bases de datos como LAION consisten en colecciones de cientos de miles de imágenes junto con una descripción textual. También proveedores de servicios de redes sociales, como Facebook, Instagram, Linkedin o Twitter/X persiguen utilizar los contenidos generados por sus usuarios como bases de datos para desarrollar modelos de lenguaje extenso y otras herramientas de IA generativa. Es innegable que estas bases de datos contendrán datos de naturaleza personal y, por lo tanto, que su creación constituirá un tratamiento de datos cubierto por el RGPD[17].

[17] No se discuten en este trabajo los problemas de aplicación geográfica del Reglamento y, en particular, hasta qué punto los elaboradores de bases de datos y los entrenadores de modelos de IA

Uno de los primeros problemas que se plantea es la identificación de una base de licitud de este tratamiento de conformidad con el artículo 6 RGPD y, en caso, de tratarse datos de categorías especiales, de conformidad con el artículo 9 RGPD[18].

Es cuestionable que bases de licitud como el propio consentimiento de los interesados (artículo 6.1.a) RGPD) o la necesidad para la ejecución de un contrato en el cual los interesados son parte (artículo 6.1.b) RGPD) sean adecuadas para los tratamientos requeridos para la elaboración de bases de datos. Muchas bases de datos se elaboran al margen de una relación contractual con los interesados y, además, a partir de técnicas masivas de *webscraping* que hacen inviable cualquier posibilidad de recabar la autorización o consentimiento de las personas afectadas.

Por ello, fuera de una previsión legal específica, la base de licitud que, de entrada, parece más adecuada para la elaboración de bases de datos a utilizar en la cadena de valor de la IA generativa es la satisfacción de intereses legítimos del compilador de la base de datos o en su caso de otro sujeto, como el desarrollador del modelo. El artículo 6.1.f) RGPD prevé que el tratamiento de datos personales será lícito si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales. Según la jurisprudencia del TJUE, este precepto establece tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero persigan un interés legítimo; segundo, que el tratamiento de los datos personales sea necesario para la satisfacción de ese interés legítimo, y, tercero, que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado en la protección de los datos[19]. En suma, será necesaria una ponderación de dere-

---

generativa situados fuera de la UE han de cumplir con el RGPD, si finalmente lo que se explota en la Unión es un sistema basado en aquellos. Véase artículo 3 RGPD.

[18] Según el artículo 9.1 RGPD constituyen categorías especiales de datos personales, dotados de un régimen jurídico más protector, aquellos «que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física».

[19] Véanse, entre otras, STJUE de 17 de junio de 2021, asunto C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA,* ECLI:EU:C:2021:492, apdo. 106; STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 106; y STJUE de 12 de septiembre de 2024, asuntos acumulados C-17/22 y C-18/22, *HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG c. Müller Rechtsanwaltsgesellschaft mbH y otros,* ECLI:EU:C:2024:738, apdo. 49. En la literatura española, véase Gil González, E. (2022). *El interés legítimo en tratamientos de datos personales.* La Ley.

chos e intereses, que plantea diversos interrogantes, entre ellos, cómo se han de valorar las expectativas razonables de los titulares de datos personales[20]; o hasta qué punto hay que considerar o no los beneficios y riesgos que puede conllevar el desarrollo futuro de modelos y sistemas de IA generativa o si únicamente se han de contemplar en la ponderación los relacionados con la propia elaboración de la base de datos, particularmente cuando las diferentes tareas son llevadas a cabo por sujetos diferentes en la cadena de valor de la IA generativa. El RGPD no descarta que el interés legítimo pueda derivar de un ejercicio de la libertad de empresa reconocida en el artículo 16 CDFUE y, por ello, es irrelevante de entrada que tanto la elaboración de la base de datos como su uso posterior para entrenar modelos de IA generativa tengan una finalidad comercial. Ahora bien, hay que tener en cuenta que muchas de las bases de datos que se están utilizando para entrenar modelos de IA generativa han sido elaboradas por entidades sin ánimo de lucro con finalidades de investigación científica[21].

Por otra parte, si la base de datos incluye categorías especiales de datos, será necesario contar con una de las bases de licitud previstas en el artículo 9 RGPD[22]. Este precepto no prevé específicamente una base de licitud basada en la satisfacción de los intereses legítimos del responsable del tratamiento o de un tercero. Por ello, de entrada, en la elaboración de las bases de datos,

---

[20] Véase considerando 47 RGPD.

[21] Véanse artículos 9.2.j) y 89 RGPD.

[22] Obsérvese que el RIA solamente se refiere a la posibilidad de tratar datos de categorías especiales de un modo doblemente limitado: la previsión cubre únicamente sistemas de IA de alto riesgo y para la finalidad específica de detección y corrección de sesgos. Véase artículo 10.5 RIA: *«En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes: a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos; b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización; c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas; d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos; e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior; f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos».*

el responsable deberá adoptar las medidas técnicas necesarias para evitar la recopilación de datos sensibles no relevantes, por ejemplo, implementado filtros que impidan la copia de determinadas categorías de datos o la no inclusión en las tareas de *scraping* de determinadas páginas web que previsiblemente contengan datos sensibles[23].

La adopción de tales medidas puede contribuir a evitar la ilicitud del tratamiento. El derecho a la protección de los datos personales no es un derecho absoluto y han de considerarse también las posibilidades del responsable para reducir el impacto negativo de sus actividades: no resulta viable y óptimo, como ha señalado el TJUE, que un buscador de internet elimine todos los datos de categorías especiales antes de mostrar sus resultados[24]. A pesar de las diferencias, esta consideración en relación con los buscadores de internet podría llegar a predicarse de las bases de datos elaboradas y utilizadas en el ámbito de la IA generativa. En cualquier caso, ha recordado el TJUE, el responsable deberá reaccionar frente al ejercicio de derechos por parte de los interesados frente al tratamiento de sus datos sensibles.

Por otra parte, el artículo 9.2.e) RGPD legitima los tratamientos referidos a datos personales que el interesado ha hecho manifiestamente públicos. Con todo, habrá que valorar, caso por caso, si los usuarios en cuestión de un sitio web o de una aplicación que introdujeron voluntariamente datos sensibles, habían consentido explícitamente, sobre la base de una información expresa facilitada por ese sitio o esa aplicación antes de tal introducción o activación, que dichos datos podrían ser visualizados por cualquier persona que tuviera acceso al citado sitio o a la referida aplicación[25]. Es dudoso, además, que las expectativas razonables de los usuarios puedan referirse al mismo tiempo a la aceptación de que terceros puedan elaborar bases de datos con su información y que estas puedan servir luego para entrenar modelos de IA generativa.

La enorme cantidad de datos tratados por medios automáticos las más de las veces entra en conflicto con el modelo individualista establecido en el sistema europeo de protección de datos europeos, que confía en una identificación de los diferentes datos tratados y la salvaguardia de los derechos de los individuos en relación con ellos. Hay claramente una tensión entre el número masivo de datos tratados en el ámbito de la IA generativa y el principio

---

[23] También puede resultar pertinente llevar a cabo una evaluación de impacto de conformidad con lo previsto en el artículo 35 RGPD, como medida adicional de mitigación de riesgos.

[24] STJUE de 24 de septiembre de 2019, asunto C-136/17, *GC y otros c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773, apdo. 37.

[25] STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 83.

de minimización. Ello se percibe también en las tareas de anotación llevadas a cabo en los procesos de elaboración de bases de datos. A la hora de añadir información valiosa a los diferentes datos recogidos y que también puede ser utilizada junto a estos para entrenar un modelo de IA generativa, será necesaria adoptar las medidas adecuadas para cumplir con los principios de minimización y de exactitud de los datos personales, previstos respectivamente en los artículos 5.1.c) y d) RGPD.

2.3.3. Modelo de IA generativa: entrenamiento y almacenamiento

A) Entrenamiento de modelos de IA generativa

A continuación, en la cadena de valor, encontramos el modelo propiamente dicho, que puede concebirse como un conjunto de técnicas y algoritmos, que a partir de una serie de pesos y variables puede utilizarse para obtener unos resultados. Existen tres características principales que pueden predicarse de estos modelos: escalabilidad, autonomía y opacidad.

Este modelo se entrena con una o más bases de datos, para que aprenda mecánica y autónomamente a detectar relaciones estadísticas o patrones en los datos y entre ellos. El entrenamiento de un modelo exige muchos recursos de tiempo y energía. Se entiende que el entrenamiento comporta actos de tratamiento de datos personales y, por tanto, deberá contar con una base de licitud y cumplir con los principios y los deberes que el RGPD impone a los responsables[26]. En buena medida, todo lo señalado en el apartado anterior referido a la elaboración de las bases de datos puede trasladarse al entrenamiento de los modelos de IA generativa.

Dependiendo de las técnicas de entrenamiento utilizado, es posible que los datos personales se anonimicen a partir del uso de técnicas como *differential privacy* o *federated machine learning*. La anonimización constituye un tratamiento de datos específico que requiere también de una base de licitud[27]. En cualquier caso, es importante considerar si efectivamente los datos son anonimizados o únicamente pseudonimizados.

---

[26] Véase, en general, Hacker, P. (2021). A legal framework for AI training data-from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, *13*(2), 257-301. https://doi.org/10.1080/17579961.2021.1977219.

[27] En general, la base de licitud será la satisfacción del interés legítimo del responsable del tratamiento. Ruschemeier, H. (2024). *Op. cit.*, pág. 8.

B) Almacenamiento y comunicación de modelos de IA generativa

Una de las cuestiones inciertas en este ámbito se refiere a la calificación jurídica de los actos de almacenamiento y comunicación de modelos de IA generativa como posibles tratamientos de datos personales. Se ha defendido que, después de entrenado un modelo de lenguaje extenso, el modelo no contiene ya datos personales, pues la información se conserva en un formato de *tokens* y *embeddings*, esto es, fragmentos que, después de anonimizar los datos, carecen de significado y son solo representaciones matemáticas que persiguen reflejar correlaciones entre diferentes elementos a partir de pesos y variables[28]. Se trataría de información agregada que no permitiría la identificación de un interesado[29]. Ahora bien, el hecho de que los sistemas de IA generativa puedan producir *outputs* que reproducen datos que se utilizaron en el entrenamiento del modelo[30] lleva a algunos autores a cuestionar que los modelos no contengan y no almacenen datos personales[31]. Las diferencias entre los diferentes tipos de modelos y, en particular, si están basados en transformadores o difusión, puede ser relevante en relación con el tipo de información finalmente almacenada y si efectivamente aquellos incluyen o no datos de carácter personal.

Si el modelo de IA generativa no almacena datos de carácter personal, su proveedor no deberá, por ejemplo, atender a peticiones de interesados que quieran ejercer sus derechos conforme al RGPD, por ejemplo, en relación con la supresión o rectificación de datos o la oposición al tratamiento.

---

[28] Hamburg Commissioner for Data Protection and freedom of information (2024). Discussion Paper: Large Language Models and Personal Data. https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf. Pág. 5.

[29] Sobre el concepto de dato personal y el test de la identificabilidad, véanse, en la jurisprudencia del TJUE, STJUE de 19 de octubre de 2016, asunto C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*. ECLI:EU:C:2016:779; STJUE de 20 de diciembre de 2017, asunto C-434/16, *Peter Nowak c. Data Protection Commissioner*. ECLI:EU:C:2017:994; STJUE de 8 de diciembre de 2022, asunto C-180/21, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*. ECLI:EU:C:2022:967; STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370; STJUE de 9 de noviembre de 2023, asunto C-319/22, *Gesamtverband Autoteile-Handel eV c. Scania CV AB*. ECLI:EU:C:2023:837; y STJUE de 7 de marzo de 2024, asunto C-604/22, *IAB Europe c. Gegevensbeschermingsautoriteit*. ECLI:EU:C:2024:214.

[30] Carlini, N., Tramer, F., Wallace, E., Jagielski, M. et al. (2021). Extracting Training Data from Large Language Models. *30th USENIX Security Symposium*. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting. 2633-2650; Staab, R., Vero, M., Balunović, M. y Vechev, M. (2023). Beyond Memorization: Violating Privacy Via Inference with Large Language Models. https://arxiv.org/ abs/2310.07298.

[31] Ruschemeier, H. (2024). *Op cit*. Pág. 6.

El RIA impone una serie de obligaciones a los proveedores de sistemas de IA de alto riesgo relativas a la gobernanza de datos, que en algunos casos podrán llegar a afectar a modelos y sistemas de IA generativa[32]. Además, con arreglo al artículo 53.1.d) RIA, los proveedores de GPAIMs «elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA». Dependiendo del tipo de detalle de la información suministrada, este deber puede comportar un nuevo acto de tratamiento de datos personales.

2.3.4. Desarrollo de sistemas basados en el modelo

A continuación, el modelo se puede desarrollar, esto es, puede transformarse en un servicio utilizable por terceros. Esto puede hacerse, por ejemplo, mediante una interfaz de usuario con un robot de conversación como hace ChatGPT o mediante una aplicación informática, entre otros. De entrada, el modelo se podrá utilizar para usos y finalidades muy diversas y se pueden desarrollar sistemas que se dirijan a una finalidad concreta (por ejemplo, generación de contenidos sintéticos, servicios de traducción, servicios de clasificación de imágenes, entre otros). El modelo se puede licenciar a un tercero, para que sea éste el que desarrolle los servicios específicos. De ahí que el RIA distinga entre modelos y sistemas de IA. En este sentido, según el artículo 2.1 RIA, un sistema de IA es *«un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la forma de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales»*.

El desarrollo de estos sistemas puede implicar nuevos actos de tratamiento de datos personales, en función de cómo se lleve a cabo. En muchos supuestos, las tareas de personalización y de *fine-tuning* podrán recurrir a nuevas bases de datos, en algunos casos de titularidad del propio desarrollador del sistema, y, en consecuencia, deberán contar con una base de licitud y cumplir con la normativa establecida en el RGPD.

Un problema potencial que puede plantearse es el relativo a los modelos divulgados en abierto que pueden ser desarrollados por cualquiera, sin necesidad de que el titular del modelo lleve a cabo un control o selección o reciba contraprestación alguna por la licencia. Es cuestionable que, si el desarrollador del modelo ha infringido la normativa sobre protección de datos,

[32] Véase artículo 10 RIA.

por ejemplo, al entrenar su modelo sin contar con una base de licitud, haya de responder por nuevas infracciones que puede llevar a cabo un tercero que desarrolla el modelo para integrarlo en sus productos y servicios. Ahora bien, ello no excluye, como se verá, que la responsabilidad civil derivada de sus propias infracciones normativas cubra el daño moral ocasionado a un individuo por el temor que el tercero en cuestión lleve a cabo unos usos maliciosos del modelo que puedan afectar negativamente a sus datos personales[33].

2.3.5. Utilización del sistema

A) Prompts

El modelo desarrollado o implementado puede utilizarse para producir las generaciones. En este sentido, los usuarios que tengan acceso al sistema y a los servicios que éste ofrezca pueden redactar instrucciones (*prompts*) para obtener textos, imágenes, sonidos u otros tipos de contenidos. Estos *prompts* pueden contener datos personales, tanto del propio usuario como de terceros. Además del propio funcionamiento inmediato del sistema, el desarrollador o el operador del modelo pueden llegar a tratar estos datos para otras finalidades (por ejemplo, para tareas de moderación de contenidos o para entrenar el modelo) y pueden llegar a almacenarlos o a utilizarlos para la mejora del modelo o sistema.

El primer supuesto es menos problemático. El usuario del sistema seguramente, al haberse dado de alta para ser destinatario de los servicios, habrá prestado su consentimiento a los diferentes tratamientos de sus datos personales. En otros términos, el tratamiento de datos del usuario destinatario de los servicios del sistema de IA generativa estará basado en el consentimiento de conformidad con los artículos 6.1 y 7 RGPD o, en su caso, el artículo 9.2.a) RGPD. El responsable del tratamiento habrá de adoptar todas las medidas para cumplir con sus obligaciones de responsabilidad activa de conformidad con el RGPD. En el caso de datos de terceros, el usuario no puede prestar el consentimiento en nombre del tercero y puede plantearse la duda de cuál ha de ser la base de licitud para la introducción y recogida de estos datos. En segundo lugar, en este último caso, se puede plantear el problema de la atribución de roles entre las diferentes personas implicadas y, en particular, si ha de considerarse al usuario del sistema de IA generativa que trata datos de terceros en forma de *inputs* como responsable del tratamiento único y al operador como encargado o corresponsable del tratamiento.

---

[33] Véase *infra* apdos. 3.2 y 3.3.

En particular, con arreglo a la jurisprudencia del TJUE, aunque pueda establecerse un supuesto de corresponsabilidad en el tratamiento, la calificación quedaría limitada a los actos relativos a la introducción de los datos y no a las tareas posteriores que pudiera llevar a cabo el operador[34].

B) Generación de resultados

Los sistemas de IA generativa pueden producir diferentes tipos de resultados (*outputs*). Por ejemplo, pueden obtenerse imágenes de personas sintéticas, esto es, retratos digitales de personas no reales, que se utilizan luego en la publicidad, catálogos u otras ilustraciones. Al no tratarse de personas físicas concretas, estas imágenes no comportarán comunicación de datos personales.

En otras ocasiones, los resultados ofrecidos por un sistema de IA generativa pueden incluir datos personales. Por ejemplo, un usuario puede solicitar información acerca de él mismo y obtener una información incorrecta o que puede afectar a su privacidad. Aunque no necesariamente este fenómeno responde a que el modelo se entrenó con datos personales del afectado, en muchos casos esto será así[35]. En este último caso, se habla de "memorización" o *overfitting*, esto es, la posibilidad que, de algún modo, las generaciones producidas por un sistema repliquen datos que se utilizaron en el entrenamiento del modelo subyacente. En la literatura técnica se han descrito diferentes razones que pueden contribuir a este fenómeno, como limitaciones en la base de datos utilizada para entrenar el modelo, duplicados y otros tipos de copias de datos incluidas en la base empleada para entrenar el modelo, la propia complejidad del modelo, o datos de baja calidad que el modelo no puede distinguir de otros relevantes.

Sea como sea, la generación de estos resultados y su puesta a disposición suponen un acto de tratamiento de datos personales. Entre otros aspectos,

---

[34] En este sentido, véanse STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH /Facebook Ireland Ltd/Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*. ECLI:EU:C:2018:388; STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyskunta*. ECLI:EU:C:2018:551*;* STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629; y STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcijak*. ECLI:EU:C:2023:949.

[35] En la literatura técnica, véanse, entre otros, Carlini, N., Hayes, J., Nasr, M., Jagielski, M., Sehwag, V., Tramèr, F., Balle, B., Ippolito, D., y Wallace, E. (2023). Extracting Training Data from Diffusion Models. *ArXiv, abs/2301.13188*.; El-Mhamdi, E., Farhadkhani, S., Guerraoui, R., Gupta, N., Hoang, L.N., Pinot, R., y Stephan, J. (2022). On the Impossible Safety of Large AI Models. *ArXiv, abs/2209.15259*; y Gupta, M., Akiri, C., Aryal, K., Parker, E., y Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access, 11*, 80218-80245.

pueden destacarse los derechos que corresponden al usuario frente al operador del sistema de IA: el derecho de acceso (artículo 15 RGPD); el derecho de rectificación (artículo 16 RGPD) y el derecho de supresión (artículo 17 RGPD).

La producción de resultados por los sistemas de IA generativa también puede llegar a inferir y revelar datos de categorías especiales. El TJUE ha señalado que el tratamiento de datos personales por parte del operador de una red social en línea como Facebook, consistente en la recogida, mediante interfaces integradas, cookies o tecnologías de almacenamiento similares, de los datos resultantes de la consulta de esos sitios y aplicaciones, así como de los datos introducidos por el usuario, en la puesta en relación del conjunto de esos datos con la cuenta de la red social de este y en la utilización de dichos datos por el operador comporta un tratamiento de categorías especiales de datos personales (artículo 9.1 RGPD)[36]. No es descartable que ello también ocurra con los servicios de generación de *outputs* mediante IA generativa.

Es habitual que los desarrolladores de modelos de IA generativa utilicen los diferentes *outputs* producidos como datos sintéticos que pueden añadirse a sus bases de datos para ser utilizados en nuevos entrenamientos u otras tareas de corrección de errores y mejora de calidad. Previsiblemente, si estos datos sintéticos incluyen datos personales, estos usos comportarán nuevos tratamientos, para los cuales el responsable deberá cumplir con las disposiciones establecidas en el RGPD.

Podemos destacar tres problemas adicionales con los resultados generados por sistemas de IA generativa. El primero de ellos se refiere a la generación de alucinaciones o resultados incorrectos. Es posible que un resultado generado incluya información falsa, incorrecta, insuficiente o desfasada sobre un individuo. Ello puede deberse, por ejemplo, a que el modelo fue entrenado con datos antiguos, que no reflejan cambios acaecidos más recientemente. En consecuencia, puede transgredirse el principio de exactitud (art. 5.1.d) RGPD). Deberán ofrecerse vías a los posibles afectados para ejercer su derecho de rectificación conforme al artículo 16 RGPD. El segundo de los problemas se refiere a la generación de resultados especialmente dañinos para derechos de la personalidad de un individuo y, en particular, de resultados sintéticos que, por sus características, puedan constituir intromisiones ilegítimas en sus derechos al honor, intimidad o propia imagen. Un ejemplo de ello serán las denominadas ultrasuplantaciones (*deepfakes*). Con arreglo al artículo

---

[36] STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537, apdo. 73. Véase también STJUE de 1 de agosto de 2022, asunto C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija,* ECLI:EU:C:2022:601.

3.60 RIA, estas se definen como *«un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos»*. Aunque el RIA establece únicamente deberes de transparencia (art. 50.4 RIA), si las ultrasuplantaciones causan daños a una persona física, se plantea la cuestión acerca del fundamento de la pretensión indemnizatoria[37]. El tercer problema concierne a la posterior utilización del *output* obtenido: si este se llega a emplear para la adopción de decisiones solamente automatizadas, sin supervisión humana, resultará de aplicación lo establecido en el artículo 22 RGPD.

Por último, puede destacarse que la producción de resultados mediante IA generativa relacionados con un individuo puede constituir un indicio de que el modelo fue entrenado con datos personales de aquel. Si bien este individuo debe poder ejercer sus derechos previstos en los artículos 13 a 22 RGPD, es muy probable que sus pretensiones no sean factibles. Por ejemplo, es dudoso que pueda ejercerse de forma efectiva un derecho de supresión o al olvido[38] o que se objete a determinados tratamientos llevados a cabo en el desarrollo de los modelos y sistemas de IA generativa. Ello se debe a que no es factible económicamente proceder a una supresión de datos personales en una base de datos para luego entrenar de nuevo el modelo con el objetivo de que no obtenga información de tales datos.

2.3.6. Otras tareas

Un modelo de IA generativa puede ser objeto de ajustes, corrección de deficiencias o evitación de algunos tipos de resultados. Esto es, los responsables del sistema pueden llevar a cabo tareas de moderación de los contenidos generados por el sistema, por ejemplo, para evitar que sean infractores de derechos o ilícitos de algún otro modo. El ajuste puede acarrear nuevos entrenamientos del modelo, por ejemplo, con nuevas bases de datos o bases modificadas o purgadas. También, en la cadena de valor, el desarrollador de un sistema de IA generativa puede decidir emprender tareas para su alineación, esto es, un refinamiento de éste para cumplir con determinados objetivos de calidad.

Todas estas tareas pueden implicar nuevos usos de datos personales y, por ende, de actos de tratamiento cubiertos por el RGPD. Con arreglo al principio de minimización y de privacidad desde el diseño, resulta recomendable evitar

---

[37] Véase *infra* apartado 3.5.

[38] Véase, por ejemplo, Chang, C. (2024). When AI Remembers Too Much: Reinventing The Right To Be Forgotten For The Generative Age. *Washington Journal of Law and Technology and the Arts, 19*(3) 22-45.

el uso de datos personales, especialmente, si se pueden realizar estas tareas con datos sintéticos o con datos totalmente anonimizados.

3. CUESTIONES Y PROBLEMAS SOBRE LA REPARACIÓN DE DE DAÑOS

3.1. Introducción: el artículo 82 RGPD como fundamento de responsabilidad civil

El desarrollo y funcionamiento de los modelos y sistemas de IA generativa pueden comportar la comisión de diversas infracciones normativas en el ámbito de la protección de datos personales: hay un riesgo de que los tratamientos de datos personales implicados no siempre cumplirán con lo establecido en el RGPD. Ello dependerá, en buena medida, primero, de cómo las agencias y tribunales vayan construyendo progresivamente el entendimiento acerca de las implicaciones que despliega el derecho de protección de datos en la IA generativa y si son más o menos estrictos y, segundo, de las propias características de cada sistema y modelo. Cada caso deberá examinarse individualmente por cuanto habrá desarrolladores y operadores que de buen inicio habrán invertido más esfuerzos y recursos en hacer sus productos y servicios más respetuosos con la normativa protectora de los datos personales (protección de datos desde el diseño y protección por defecto (artículo 25 RGPD)) y otros menos cuidadosos que habrán adoptado decisiones más arriesgadas. En cualquier caso, es posible que en el desarrollo y funcionamiento de los modelos y sistemas de IA generativa se causen daños y perjuicios a usuarios y terceros.

El artículo 82 RGPD establece un fundamento de responsabilidad para la compensación de los daños derivados de infracciones normativas del derecho de protección de datos y, por ello, es probable que en los próximos años afectados por modelos y sistemas de IA generativa recurran a este precepto para fundar al menos algunas de sus pretensiones resarcitorias y, en particular, aquellas relativas a perjuicios que formen parte del ámbito de protección de las normas infringidas. Según el artículo 82.1 RGPD, *«[t]oda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos»*[39].

[39] Para una discusión del precepto, véase Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, 5(4), 53-87.

En los dos últimos años, el TJUE ha dictado varias sentencias en las cuales ha ido interpretando el artículo 82 RGPD y, en la actualidad, penden también varias cuestiones prejudiciales, que, luego de resueltas, acabarán perfilando cómo ha de funcionar la reparación de los daños derivados de infracciones normativas en materia de protección de datos personales. Hasta la fecha, el Tribunal ha sido muy claro en señalar que este precepto incluye unos requisitos cumulativos que han de acreditarse para que prospere una pretensión indemnizatoria basada en él: la comisión de una infracción del Reglamento, el padecimiento de daños y perjuicios materiales o inmateriales, y una relación de causalidad entre la infracción y dichos daños y perjuicios[40]. Esta comprensión jurisprudencial va a tener que aplicarse en los próximos años a las diferentes pretensiones indemnizatorias que ejerzan individuos que consideren que sus datos personales hayan sido afectados por modelos y sistemas de IA y que con ello hayan sufrido daños.

El incremento en el uso de modelos y sistemas de IA generativa y sus tratamientos de datos personales comportarán con alta probabilidad algunos retos para la gestión de los daños y su compensación. Hay, al menos, tres cualidades que podrán acompañar a los daños y perjuicios asociados con modelos y sistemas de IA generativa y modelos similares: su carácter masivo, pues es probable que una misma operación o un mismo sistema afecten a grandes grupos de población; su naturaleza cumulativa, pues si bien el impacto inicial sobre la esfera de un individuo puede ser mínimo, la escalabilidad, repetición y amplificación que permiten las tecnologías digitales resultan en un incremento de su alcance y gravedad[41]; y la posibilidad de que se proyecten reticularmente, esto es, que, aprovechando los efectos de red (*network effects*) que presentan muchas tecnologías de inteligencia artificial, afecten a sujetos diferentes a la víctima primaria[42]. Estas características anticipan una potencial avalancha de reclamaciones indemnizatorias para las cuales el sistema de responsabilidad civil extracontractual, y, en particular, el artículo 82 RGPD, no está seguramente bien equipado[43]. Otros retos derivarán de la implicación de varios

---

[40] STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370, apdo. 32; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 34; y STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*, ECLI:EU:C:2024:536, apdo. 22.

[41] Famularo, J. (2023). Platform-Related Harms., *Yale-Wikimedia Initiative on Intermediaries & Information*, 1-14. https://law.yale.edu/sites/default/files/area/center/isp/documents/platformrelatedharms_ispessayseries_2023.pdf. Págs. 8-9.

[42] Es lo que los profesores Anna Beckers y Gunther Teubner han denominado "daños por interconectividad" (*interconnectivity damages*). Véase Beckers, A., y Teubner, G. (2021). *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds*. Hart, 161-162.

[43] Sobre ello, Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Álvarez Lata, N. (2024). *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*. APPDC-Aranzadi. 621-688.

agentes en la cadena de valor de la IA generativa y de los riesgos relacionados con la ciberseguridad.

3.2. Daños mínimos y de bagatela

El carácter masivo del impacto negativo que pueden desplegar los modelos y sistemas de IA generativa en miles, sino millones, de individuos cuyos datos personales fueron utilizados para tareas de entrenamiento sin contar con una base de licitud o infringiendo de otro modo el RGPD puede comportar que un gran número de víctimas y otros perjudicados acaben sufriendo daños de diversa índole. Acaso en la esfera individual, el daño puede ser mínimo. De hecho, es asumible que el valor patrimonial de los propios datos personales es ínfimo o nulo: los datos de un sujeto específico no presentan un valor idiosincrático para quien quiere elaborar una gran base de datos o entrenar un modelo de IA generativa; son fungibles con otros y, por ello, prescindibles. El responsable del tratamiento está interesado únicamente en disponer de cuantos más datos mejor. Por otra parte, el daño moral de conocer que los datos de uno han sido incluidos en una base de datos utilizada luego para entrenar un modelo de IA generativa también puede ser escaso o limitado. En suma, las pretensiones indemnizatorias en este sector pueden serlo por cantidades modestas.

En determinados ordenamientos y regímenes particulares, hay reglas que impiden la reparación de estos daños insignificantes, por ejemplo, mediante el establecimiento de umbrales (*de minimis*). El objetivo principal es evitar una avalancha de reclamaciones de escasa cuantía (*Bagatelklagen*) que saturen el sistema judicial de responsabilidad civil extracontractual y, por ello, suelen ponerse límites a perjuicios que suelen presentarse de forma dispersa y alcanzar a una clase más o menos indeterminada de víctimas. Así ocurre, por ejemplo, con algunos supuestos de daño moral autónomo y de daños económicos puros[44].

En aplicación del artículo 82 RGPD, el TJUE ha señalado, sin embargo, que el principio de reparación efectiva fundamenta el derecho a ser compensado por el daño realmente sufrido, con independencia de su cuantificación. Esta fue una de las primeras cuestiones resueltas por el TJUE en la primera de las sentencias dictadas en interpretación del artículo 82 RGPD, la de 4 de mayo de 2023, en el asunto *Österreichische Post*[45].

Los hechos del caso fueron los siguientes. «Österreischische Post», una compañía austríaca dedicada a la edición de listines telefónicos y venta de ba-

[44] Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Especialmente, pp. 664-672.

[45] STJUE de 4 de mayo de 2023, asunto C-300/21, *UI v. Österreichische Post AG*, ECLI:EU:C:2023:370.

ses de datos postales, utilizaba desde el 2017 un algoritmo para identificar las afinidades políticas de ciudadanos de aquel país. Su objetivo era confeccionar grupos de sujetos para luego comercializarlos a anunciantes.

Un ciudadano austríaco descubrió que la compañía había inferido con este algoritmo su afinidad política con un determinado partido de aquel país. Si bien este dato inferido no fue comunicado a terceros, ni utilizado con ninguna finalidad, el individuo consideró que la atribución de esta afinidad política le había supuesto «una importante contrariedad, una pérdida de confianza y un sentimiento de humillación». Por ello, inició un proceso judicial en el cual solicitó que se cesara en el tratamiento de sus datos y reclamó una indemnización de 1.000 euros en concepto de daño moral. Los tribunales internos denegaron la pretensión indemnizatoria al considerar que, en el derecho austríaco, se exige un determinado umbral de gravedad para que pueda prosperar y que no era suficiente con los meros sentimientos negativos experimentados por el actor. El Tribunal Supremo austríaco (*Oberster Gerichtshof*) suspendió el procedimiento y planteó diferentes cuestiones prejudiciales al TJUE. En particular, inquirió acerca de si la exigencia de un umbral mínimo de gravedad era compatible o no con el artículo 82 RGPD.

Para el TJUE, el derecho a indemnización establecido en el artículo 82 RGPD no está supeditado a que los daños y perjuicios considerados alcancen un determinado umbral de gravedad. Para el Tribunal, condicionar la indemnización a haber superado un determinado límite cuantitativo o cualitativo podría afectar a la aplicación coherente y uniforme del régimen jurídico armonizado en el RGPD, ya que jueces y tribunales de diferentes tribunales podrían adoptar soluciones diversas[46].

Si bien las reglas sobre cuantificación de los importes indemnizatorios corresponden al derecho nacional de los EE.MM. en virtud del principio de autonomía procesal, las autoridades nacionales han de respetar los principios de equivalencia y efectividad del derecho europeo. Una regla *de minimis*, que estableciera únicamente la indemnizabilidad de los importes que superaran determinado importe, podría llegar a transgredir el principio de efectividad, ya que podría llegar a hacer imposible en la práctica o excesivamente difícil el ejercicio de los derechos establecidos en el artículo 82 RGPD, que consagra una regla de reparación integral del daño y permite la compensación de una «indemnización total y efectiva por los daños y perjuicios sufridos» (Considerando 146 RGPD)[47]. El TJUE ha reiterado esta doctrina en otros asuntos[48].

---

[46] Apdo. 49.

[47] Apdos. 56-58.

[48] STJUE de 14 de diciembre de 2023, asunto C-456/22, *VX, AT c. Gemeinde Ummendorf*, ECLI:EU:C:2023:988, apdo. 23; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*,

En consecuencia, es posible que las infracciones del derecho de protección de datos cometidas en el campo de la IA generativa lleven aparejadas la causación de daños masivos a un conjunto muy elevado de víctimas y que una porción no desdeñable de ellas entable pleitos para solicitar una indemnización pecuniaria relativamente baja o simbólica. Esta situación habrá de conllevar problemas de gestión del sistema de reparación. En otros términos, el artículo 82 RGPD no impide que cualquier afectado que pueda acreditar un daño mínimo relacionado con la infracción de normas del RGPD y ocurrido en el desarrollo y funcionamiento de un modelo o un sistema de IA generativa pueda formular una demandada de responsabilidad civil antes los juzgados y tribunales competentes.

3.3. Indemnizabilidad del temor

El concepto de daño indemnizable con arreglo al artículo 82 RGPD es muy amplio y cubre, de entrada, cualesquiera menoscabos patrimoniales o no patrimoniales sufridos efectivamente por una persona física a raíz de un comportamiento infractor de la normativa protectora de los datos personales[49]. El TJUE ha restringido doblemente este alcance extenso. Primero, ha señalado que no puede predicarse un daño *per se* de una mera infracción normativa[50]: la víctima habrá de acreditar el perjuicio efectivamente sufrido como un requisito diferente e independiente al de la prueba de la infracción normativa

ECLI:EU:C:2024:288, apdo. 36; y STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531, apdo. 46.

[49] Considerando 75 RGPD: *«Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados»*.

[50] STJUE de 4 de mayo de 2023, asunto C-300/21, *UI v. Österreichische Post AG,* ECLI:EU:C:2023:370, apdo. 42; STJUE de 25 de enero de 2024, asunto C-687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72, apdo. 61; STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 43; y STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT c. PS GbR y otros*, ECLI:EU:C:2024:536, apdo. 28.

cometida, sin que ello obste a que pueda contar con mecanismos procesales que contribuyan a la acreditación de aquel en el pleito. Y, segundo, también ha indicado el TJUE que no sucede un daño automáticamente por la infracción del derecho a la protección de datos o por la infracción de una norma del RGPD que atribuye un derecho o potestad a un individuo[51]. El daño es, pues, algo más que la mera vulneración de un derecho.

Una de las cuestiones más interesantes decididas por el TJUE se refiere a la indemnizabilidad del temor por un mal uso potencial de los datos personales de un sujeto. Pueden identificarse escenarios en los cuales, después de un hecho accidental que no genera perjuicios inmediatos, el impacto que experimentan los individuos queda reducido al miedo o la angustia de que en el futuro puedan sufrir un daño cierto. Por ejemplo, una brecha de seguridad en una base de datos y una pérdida de control sobre los mismos puede llevar a una persona a temer que finalmente aquellos se revelen a terceros o que se usen de forma ilícita. En el ámbito de la IA generativa pueden también identificarse supuestos de daños derivados de la mera exposición a un riesgo. Un ejemplo de ello sería el de la angustia generada por conocer que un modelo entrenado ilícitamente con los propios datos puede llegar a ser desarrollado con fines maliciosos o pueda llegar a producir *outputs* dañosos en el futuro. Obsérvese que la mera infracción inicial cometida por el desarrollador del modelo –por ejemplo, no contar con una base de licitud válida– es insuficiente por ella misma para generar responsabilidad civil y que es necesaria la acreditación de un daño real y efectivo. El mero entrenamiento de un modelo con datos personales no genera automáticamente un daño patrimonial u otro no patrimonial a todas las víctimas, pero, en aplicación de la jurisprudencia del TJUE, algunas de ellas, ante la posibilidad de que sus datos puedan llegar a ser afectados en el futuro, pueden haber experimentado una situación de miedo, angustia o desamparo tal que revele el sufrimiento real de un daño moral.

En el último de los asuntos sobre esta cuestión –la Sentencia de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*[52]–, el TJUE se enfrentó a un supuesto de pérdida hipotética de control sobre unos datos personales. Los hechos del caso fueron los siguientes: dos clientes de una asesoría

---

[51] STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288, apdo. 37. Sobre la compensación de una posible vulneración del derecho de acceso, pende actualmente un asunto ante el TJUE. Se trata del asunto C-526/24, derivado de la petición de decisión prejudicial formulada el 31 de julio de 2024 por el *Amtsgericht* Arnsberg (Tribunal de lo Civil y Penal de Arnsberg, Alemania), en un caso con las partes siguientes: *Brillen Rottler GmbH & Co c. KG*.

[52] STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536. Para un comentario a la sentencia, véase Carrasco Perera, A. (Septiembre de 2024). El daño que consiste en no saber si se ha producido o no una infracción y un perjuicio de datos personales. *GA-P Análisis*. https://ga-p.com/publicaciones/el-dano-que-consiste-en-no-saber-si-se-ha-producido-o-no-una-infraccion-y-un-perjuicio-de-datos-personales/.

fiscal en Alemania informaron a sus empleados de un cambio de dirección postal, que fue correctamente modificado en sus bases de datos. A pesar de haber recibido varios correos en el nuevo domicilio, la carta con las declaraciones fiscales del año 2019 fue enviada al domicilio anterior, cuyos nuevos residentes abrieron por error y, finalmente, entregaron a unos allegados de los demandantes. No se sabe del cierto y no se pudo acreditar en el pleito que en el sobre abierto figurara, además de la declaración, documentación adicional con datos personales de los actores tales como fechas de nacimiento, datos de los hijos, profesiones y lugares de trabajo, pertenencia a una comunidad religiosa o la condición de persona con discapacidad de un miembro de su familia.

Los clientes demandaron a la asesoría fiscal y solicitaron una indemnización de 15000 euros por el daño moral sufrido a consecuencia de la divulgación de sus datos personales a terceros. El Tribunal de lo Civil y Penal de Wesel (*Amtsgericht* Wesel) decidió suspender el procedimiento y plantear varias cuestiones prejudiciales al TJUE. Entre ellas, inquirió acerca de «si el temor a que los datos personales lleguen a manos de personas no autorizadas puede constituir, por sí solo, un daño inmaterial capaz de generar un derecho a una indemnización pecuniaria en virtud del artículo 82 del RGPD»[53].

El TJUE señala que «[l]a pérdida de control sobre los datos personales, incluso durante un breve período de tiempo, puede causar al interesado "daños y perjuicios inmateriales" […] que den lugar a un derecho a indemnización, siempre que dicho interesado demuestre que ha sufrido efectivamente tales daños y perjuicios, por mínimos que sean»[54]; y que no basta simplemente con alegar el temor para acreditar el daño efectivamente sufrido[55].

Con anterioridad, el TJUE ya se había pronunciado en dos ocasiones acerca de la indemnizabilidad del temor. En el primero de los casos –el asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*[56] –, el miedo a indemnizar se producía a consecuencia de un ataque informático por un *hacker* que había comprometido la seguridad de una base de datos dependiente del Ministerio búlgaro de finanzas y se había hecho con datos personales de millones de ciudadanos: cientos de ellos entablaron acciones para ser compensados por la angustia de saber que sus datos podían llegar a ser utilizados con fines maliciosos en el futuro. En el segundo de los casos –el asunto C-687/21, *BL c.*

---

[53] Apdo. 15.
[54] Apdo. 33.
[55] Apdo. 35.
[56] STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986.

MediaMarktSaturn[57]–, el TJUE hubo de enfrentarse con las bases sentadas en el caso anterior a una demanda que es punto menos que un despropósito: el actor acudió a un centro comercial donde compró un electrodoméstico, que había de recoger luego en un mostrador al efecto. Otro cliente acudió al mostrador y recogió por error el electrodoméstico comprado por el primero de ellos, junto con el contrato y demás documentación que incluía datos personales de este, tales como su nombre, teléfono y dirección postal. En una media hora se pudo recuperar el electrodoméstico y la documentación, y era muy probablemente que el segundo cliente no hubiera tenido acceso efectivo a los datos. A pesar de ello y aunque el vendedor se había ofrecido a entregar el aparato sin coste en su domicilio, el afectado formuló demanda y exigió una indemnización por el daño moral resultante de la exposición al riesgo de que su información hubiera podido llegar a ser conocida por terceros o copiada y utilizada más adelante. El TJUE recuerda que las sensaciones de temor ante el riesgo de una futura utilización de los datos pueden constituir daños no patrimoniales, pero que incumbe al afectado acreditar su concurrencia. Además, el Tribunal indica que *«[…] el riesgo puramente hipotético de un uso indebido por parte de un tercero no autorizado no puede dar lugar a indemnización alguna. Ello será el caso cuando ningún tercero hubiera tenido conocimiento de los datos personales en cuestión»*[58].

Los tres casos resueltos por el TJUE hasta la fecha acerca de la indemnización del temor sufrido por experimentar el riesgo de un daño futuro derivado de la potencial utilización maliciosa de los datos personales propios invitan a formular varias cuestiones, que podrán llegar a plantearse en los años próximos en las controversias que surjan en el campo de la IA generativa.

La primera de ellas se refiere a la identificación del riesgo frente al que se experimenta el temor. El Tribunal únicamente ha señalado que el riesgo puramente hipotético no puede justificar una indemnización por el temor sufrido. Por lo tanto, a efectos de la pretensión indemnizatoria, será necesario identificar un riesgo real. En otros términos, será necesario establecer que algún tercero o grupo de terceros ha obtenido conocimiento de los datos personales en cuestión, pues sin tal conocimiento el riesgo es meramente hipotético. Hay varias críticas que pueden formularse a esta apreciación que hace la jurisprudencia del TJUE: (i) Uno puede experimentar el temor con independencia de si el riesgo es real o inexistente o hipotético: un sujeto puede sufrir miedo y ansiedad si efectivamente conoce que terceros han tenido acceso a sus datos o si cree que ello es posible pero lo ignora. Saber *ex post* que nadie tuvo acce-

[57] STJUE de 25 de enero de 2024, asunto C-687/21, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72.

[58] Apdo. 68 (traducción del autor: la STJUE no está disponible en español).

so a los datos puede poner punto final al temor, pero no elimina que en un periodo más o menos largo de tiempo aquel individuo habrá experimentado el temor. Acaso el Tribunal podría clarificar que, en este último supuesto, el temor constituye un riesgo general de la vida o un daño que el afectado tiene el deber jurídico de soportar; (ii) Señala el TJUE que no procede la compensación del temor cuando ningún tercero hubiera tenido conocimiento de los datos personales, pero no aclara qué ha de entenderse por «conocimiento». En particular, desconocemos si ha de tratarse de un conocimiento efectivo, que puede resultar muy difícil de acreditar por la víctima, o de una posibilidad razonable de conocer los datos; y (iii) el TJUE no parece distinguir los tres casos resueltos hasta la fecha sobre indemnizabilidad del temor y ofrece una solución común a todos ellos, cuando hay un factor que puede convertir el riesgo en cuestión en jurídicamente relevante: un comportamiento doloso o intencional que incrementa irrazonablemente el riesgo de un mal uso frente a un descuido o a un error que resulta únicamente en un potencial acceso inadecuado a los datos pero que no parece contribuir a un incremento irrazonable del riesgo. No parece que todos estos casos hayan de recibir el mismo tratamiento jurídico.

La segunda cuestión que plantea la jurisprudencia del TJUE hace referencia al umbral de dolor o de temor requerido para fundar un derecho a ser compensado. Si el temor es el daño moral indemnizable, el TJUE recuerda que no puede aplicarse una regla *de minimis* y que cualquier daño, por pequeño que sea, puede ser objeto de compensación. La víctima deberá acreditar la realidad de este dolor, sin que baste la mera alegación de haberlo experimentado. La víctima deberá pues aportar elementos de prueba suficiente para acreditar haber sufrido este temor[59]. Un problema con este tipo de daño inmaterial deriva del hecho que las personas experimentamos el miedo y el temor de modos diferentes: hay personas más aprehensivas que otras y personas más tolerantes del dolor. El temor es pues, en buena medida, un daño idiosincrático. Por ello, la prueba dependerá de factores externos y objetivos. Si no hay documentos o testigos que acrediten la realidad del dolor, el principal elemento de prueba acabará siendo la gravedad de los hechos e inferir el daño *in re ipsa*. En consecuencia, de algún modo, no se acabarán indemnizando las situaciones menos graves: una regla *de minimis* se acabará aplicando por la puerta de atrás.

---

[59] STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986: «[…] cuando una persona que solicita una indemnización por este motivo invoca el temor de que en el futuro se produzca un uso indebido de sus datos personales como consecuencia de dicha infracción, el órgano jurisdiccional que conozca del asunto deberá comprobar que ese temor puede considerarse fundado, habida cuenta de las circunstancias específicas del caso y del interesado» (apdo. 85).

La tercera cuestión acerca de esta línea jurisprudencial del TJUE se refiere a las consecuencias que ha de desplegar la concreción futura del riesgo, esto es, de la materialización de un daño a resultas del uso ilícito de los datos personales por un tercero en un momento más o menos alejado en el tiempo. En otros términos, el temor que padecía la víctima a que sus datos se utilizaran se convierte en realidad y estos finalmente son divulgados, utilizados para obtener determinados beneficios, manipulados o de algún otro modo empleados por un tercero. Con arreglo a la jurisprudencia del TJUE, hay que distinguir dos tipos de daños en estas situaciones: el temor experimentado efectivamente por la víctima y el daño resultante del mal uso posterior de los datos (que podrá ser patrimonial o no patrimonial)[60]. En otras palabras, el TJUE permite la indemnización del temor como tal, pero no se refiere a la compensación de un daño probabilístico, definido como el daño futuro causado por el tercero multiplicado por la probabilidad de que ocurra. Son pues dos daños diferentes causados por hechos y sujetos diferentes. El Prof. Ángel Carrasco ha explicado que el TJUE admite la indemnización del temor porque ya hay daño pero que no se refiere a la indemnizabilidad de un daño temido, para el cual el derecho en ocasiones «ha previsto una especie de *cautio damni infecti* mediante la que el juez ordena al demandado (si así se aprecia) prestar una caución»[61]. Al tratarse de daños diferentes, una vez materializado el riesgo, el responsable del tratamiento demandado que satisfizo la indemnización a la víctima no ostentará ningún derecho de repetición o reembolso contra quien hubiera después usado ilícitamente los datos personales.

3.4. Brechas de seguridad

Los modelos de lenguaje extenso y, por ello, los modelos de IA generativa pueden ser objeto de varias acciones maliciosas que comprometan su ciberseguridad[62]. En primer lugar, pueden destacarse los *privacy attacks* o *information*

---

[60] Por ejemplo, en el asunto *Scalable Capital*, el TJUE distingue dos tipos de perjuicios diferentes: el posible daño directo derivado de una pérdida de datos a partir de un ciberataque y el posible daño futuro derivado de una usurpación o fraude de identidad. En el caso, terceros no identificados accedieron maliciosamente a datos personales y otros relacionados con el funcionamiento de una *trading app* o aplicación informática de negociación con valores, gestionada por la sociedad alemana Scalable Capital. Véase STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531, apdos. 54-58.

[61] Carrasco Perera, A. (Septiembre de 2024). *Op. cit.*, pág. 4.

[62] Para una descripción general de los diferentes riesgos asociados a la seguridad de la información en el campo de la IA generativa, véase Bundesamtes für Sicherheit in der Informationstechnik (Abril de 2024). Generative AI Models Opportunities and Risks for Industry and Authorities. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4.

extraction attacks: su objetivo es obtener información acerca de la arquitectura de un modelo para reconstruirlo totalmente o en parte o conseguir información sobre los datos utilizados en su entrenamiento. Ello puede realizarse, por ejemplo, mediante consultas acerca de si determinada información fue utilizada o no (*membership inference attacks*) o por medio de otros *prompts*. A partir de diferentes técnicas, un tercero puede llegar a obtener datos personales que fueron utilizados en el entrenamiento de un modelo, datos personales añadidos como *inputs* por un usuario durante su utilización de un sistema de IA generativa, y también datos personales contenidos en las generaciones o *outputs* producidos por el sistema. Por otra parte, hay riesgos de reidentificación de datos anonimizados.

La seguridad de un modelo o sistema de IA generativa también puede afectarse mediante *evasion attacks*, que persiguen alterar y manipular el comportamiento de aquellos o evadir medidas de protección adoptadas por sus desarrolladores. Así, pues, es posible que un tercero mediante determinadas técnicas pueda eludir los diferentes filtros y mecanismos de protección implementados para que un sistema no produzca determinados resultados. En otros términos, aunque el desarrollador de un sistema de IA generativa hubiera adoptado filtros para que determinados datos personales sensibles no pudieran ser revelados por medio de *outputs*, un tercero sofisticado podría llegar a sortear tales barreras y obtener los datos en cuestión. Entre las técnicas utilizables, destacan las llamadas *prompt injections*.

Otro grupo de problemas de ciberseguridad tiene que ver con los denominados *poisoning attacks*. Se trata de acciones que persiguen alterar o manipular características del modelo como los datos de entrenamiento o su propia arquitectura. En el primer caso, si se anticipa que un modelo puede entrenarse con determinadas fuentes, el «envenenamiento» pasa, por ejemplo, por una manipulación de las páginas web que se rastrean para generar la base de datos. En el segundo caso, ello puede ser más factible en casos de modelos licenciados en abierto –cuyos pesos y variables pueden ser públicos–, que pueden ser desarrollados luego por cualquier tercero y que pueden dar lugar a alteraciones maliciosas de su estructura y características.

Dados los riesgos descritos, es probable que individuos que conozcan que un determinado modelo o sistema de IA generativa ha sido objeto de un ataque que haya permitido un acceso a sus datos personales o una manipulación o alteración de estos resuelvan emprender acciones de responsabilidad civil contra el titular o desarrollador de aquel. Obsérvese que se trata de comportamientos llevados a cabo por terceros difícilmente identificables y que actúan dolosamente y, por tanto, puede plantearse la conveniencia d imputar tales daños al demandado. En otros términos, se abre la vía a acudir a criterios

de imputación objetiva para desligar o no al demandado de las pretensiones indemnizatorias o, desde una perspectiva tradicional, para identificar una interrupción del nexo causal. De hecho, el propio artículo 82.3 RGPD establece que *«[e]l responsable o encargado del tratamiento estará exento de responsabilidad […] si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios»*. No obstante, en aplicación de este precepto, puede sostenerse que el titular o desarrollador del modelo o sistema de IA generativa puede llegar a responder si no hubieran adoptado las medidas técnicas adecuadas de seguridad de la información que hubieran evitado el ataque o al menos mitigado de forma razonable su ocurrencia. Esto es, puede llegar a responder si su omisión o la adopción de medidas insuficientes ha contribuido irrazonablemente a un incremento del riesgo de ciberataque.

En relación con esta cuestión, se ha pronunciado ya el TJUE en una sentencia ya citada: la STJUE de 14 de diciembre de 2023 dictada en el asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*[63]. El caso se refería al acceso malicioso por un tercero a datos de millones de ciudadanos búlgaros que se contenían en una base gestionada por una agencia pública, dependiente del Ministerio de Finanzas, encargada de identificar y reclamar deudas públicas. Parte de esta información fue publicada luego en internet.

Cientos de ciudadanos demandaron a la agencia *Natsionalna agentsia za prihodite* (en adelante, NAP), entre ellos, la actora en el pleito del que finalmente tuvo conocimiento el TJUE. En su reclamación ante los tribunales búlgaros, la Sra. VB solicitó la cantidad de 1000 leva (aproximadamente, unos 510 euros) por el daño moral consistente en que alguien pudiera utilizar la información publicada en internet o que, gracias a ella, pudieran chantajearla, atacarla o secuestrarla.

La principal defensa de NAP consistió en afirmar que había adoptado todas las medidas técnicas necesarias *ex ante* para evitar un ciberataque como el efectivamente sufrido y *ex post* para mitigar las consecuencias negativas de este. Para el TJUE, el examen de si un responsable del tratamiento ha cumplido con sus obligaciones de seguridad con arreglo a los artículos 24.1 y 32 RGPD ha de hacerse caso por caso. Es necesario que los tribunales que decidan acerca de una pretensión indemnizatoria por los daños derivados de una brecha de seguridad aprecien si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento fueron apropiadas, teniendo en cuenta los riesgos vinculados al tratamiento y apreciando si la naturaleza, el contenido

---

[63] STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986. Para un comentario de la Sentencia, véase Martín Faba, J. M. (2024). Novedades en materia de indemnización y protección de datos personales. *Revista CESCO De Derecho De Consumo,* (49), 131-147. https://doi.org/10.18239/RCDC_2024.49.3474.

y la adopción de esas medidas están adaptados a estos riesgos y, por lo tanto, que examinen si hubo o no una infracción del RGPD[64]. Para el Tribunal, incumbe al responsable del tratamiento demandado en el proceso la carga de la prueba de acreditar que las medidas técnicas y organizativas adoptadas fueron apropiadas y que, en efecto no infringió el RGPD[65]. Ello deriva del principio de responsabilidad activa previsto en el artículo 5.2 RGPD que establece el deber de los responsables del tratamiento de demostrar que cumplen con lo previsto en el Reglamento. Aclara también el Tribunal que confiar la acreditación del carácter apropiado o inapropiado de las medidas técnicas y organizativas solo y exclusivamente a un informe pericial es contrario al principio de efectividad del derecho de la UE: un informe pericial presentado de parte o solicitado por un juez puede ser una prueba relevante, pero no siempre será necesaria y sus conclusiones pueden ser contradichas por otros tipos de pruebas[66]. Finalmente, destaca el TJUE, que, si las medidas resultan inapropiadas, ya no es posible para el responsable del tratamiento exonerarse de responder conforme a lo previsto en el artículo 82.3 RGPD: ya no es *«en modo alguno responsable del hecho que haya causado los daños y perjuicios»*, por cuanto su comportamiento contribuyó, en menor o mayor grado, a la producción de los daños.

En suma, en los pleitos de responsabilidad civil por daños derivados de problemas de seguridad de la información relacionados con la IA generativa, de seguirse esta línea jurisprudencial, se produciría una inversión de la carga de la prueba en relación con la acreditación de uno de los requisitos de la pretensión: corresponderá al responsable demandado probar que no infringió el artículo 32 RGPD y que las medidas técnicas y organizativas adoptadas para reducir o eliminar los riesgos asociados con la ciberseguridad fueron apropiadas. Por su parte, incumbirá al actor en el pleito la prueba del daño efectivamente sufrido y de la relación de causalidad.

3.5. Relaciones con otros fundamentos de responsabilidad: el caso de los *deepfakes*

Un supuesto específico de causación de daños en el campo de la IA generativa resultará de la generación y uso posterior de ultrasuplantaciones o *deepfakes*. Por ejemplo, un usuario puede utilizar un sistema de IA generativa

---

[64] Apdo. 47. El TJUE no valora la posibilidad de que la infracción normativa hubiera podido ser identificada y, en su caso, sancionada por una agencia de protección de datos y que papel tendría esta resolución en el pleito civil de reclamación de daños y perjuicios. En consecuencia, a falta de un procedimiento administrativo previo o en paralelo, la prueba de la infracción habrá de establecerse en el pleito civil (*stant-alone claims*).

[65] Apdo. 57.

[66] Apdo. 64.

para generar y luego divulgar un vídeo sintético que muestre a un individuo tomando parte en unos hechos en los cuales nunca participó o diciendo unas palabras que nunca pronunció.

Una de las cuestiones principales que se plantea en este caso –además de la posibilidad de reclamar frente al operador del sistema, por ejemplo, si el usuario que divulgó el vídeo no puede ser identificado– es el de si la víctima puede acudir a otras bases diferentes del artículo 82 RGPD para fundar su pretensión indemnizatoria. En particular, en el derecho español, se pueden señalar al menos tres fundamentos diferentes que, en función de los casos podrán llegar a alegarse: la responsabilidad civil extracontractual general recogida en los artículos 1902 y ss. CC; la responsabilidad civil derivada de delito prevista en los artículos 109-122 CP; y la responsabilidad civil por intromisiones ilegítimas en los derechos al honor, propia imagen e intimidad personal y familiar regulada en la LO 1/1982[67]. Seguramente, los actos de producción, comunicación y difusión del vídeo constituirán, a falta de una causa de exoneración, intromisiones ilegítimas en el derecho a la propia imagen de la persona cuya imagen se ha reproducido sintéticamente; además, en función del contenido del vídeo, podrán vulnerarse sus derechos al honor y a la intimidad personal; y, finalmente, puesto que para la generación del vídeo se habrán tratado datos personales de la persona afectada en varios momentos, es también posible que se hayan cometido infracciones del RGPD que lleven aparejadas la causación de un daño moral a aquella compensable con arreglo al artículo 82 RGPD.

La acción prevista en el artículo 82 RGPD es acumulable a otras acciones indemnizatorias. En este sentido, el considerando 146 RGPD señala que el régimen que prevé para la compensación de los daños y perjuicios derivados de un tratamiento de datos personales en infracción de la normativa ha de entenderse *«sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros»*[68]. Acudir al artículo 9.3 de la LO 1/1982 en lugar de a la acción prevista en el artículo 82 RGPD puede resultar atractivo para las víctimas en estos

---

[67] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115, de 14.5.1982).

[68] Sobre la compatibilidad de diferentes pretensiones indemnizatorias en el ámbito de la protección de datos personales, véanse Moreno Martínez, J.A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. Ataz López, J. y Cobacho Gómez, J.A. (Coords.) (2021). *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*. Thomson -Aranzadi, Tomo 3, 515-565; y Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución*, 34, 197-232.

casos: el precepto establece una presunción de causación de daño moral a partir de la intromisión ilegítima en uno de los derechos de la personalidad protegidos por la ley; que, además, ha sido calificada en la jurisprudencia como una presunción *iuris et de iure* que no admite prueba en contrario. En efecto, la víctima fundando su pretensión indemnizatoria en la LO 1/1982 puede ahorrarse los esfuerzos necesarios para la acreditación del daño no patrimonial resultante de un *deepfake*, que de acudir al remedio del artículo 82 RGPD habría de realizar.

Sea como fuere, surgen dos problemas que podrán llegar a discutirse en los litigios planteados en relación con la IA generativa. El primero de ellos se refiere a la posibilidad de acumulación de acciones y de obtención de indemnizaciones supracompensatorias. El TJUE ha señalado que el derecho interno puede contar con normas que permitan fijar una indemnización superior a la reparación total y efectiva de los daños cubierta por el artículo 82 RGPD[69]: : *«[…] si el Derecho nacional lo permite, el juez nacional pued[e] conceder al interesado una indemnización superior a la reparación total y efectiva prevista en el artículo 82, apartado 1, del RGPD en caso de que, habida cuenta de que el perjuicio también ha sido causado por la infracción de disposiciones de Derecho nacional […], esta última reparación no se considere suficiente o adecuada»*. En buena medida, la cuestión pasará por determinar si las normas nacionales infringidas son normas de desarrollo del RGPD o no. En el primer supuesto, la indemnización no podrá superar el principio de reparación integral del que parte el RGPD: el máximo indemnizable es el perjuicio efectivamente sufrido por la víctima y no podrán tenerse en cuenta la infracción simultánea de varias disposiciones internas para incrementar el *quantum* indemnizatorio[70]. En el segundo supuesto, parece que el TJUE admite la acumulación de diferentes pretensiones de daños y la posibilidad de obtener una indemnización superior[71]. Claramente, la acción prevista en el art. 9.3 LO 1/1982 no forma parte de una norma de desarrollo del RGPD. Un legislador nacional también podría aprobar una norma interna sobre *deepfakes* que incluyera normas sobre compensación de daños con criterios autónomos de cuantificación de daños. El segundo de los problemas afecta a la posibilidad de que la utilización de un remedio o fundamento diferente previsto en el derecho interno de un Estado miembro llegue a transgredir los principios de efectividad y equivalencia del Derecho de la UE. Habrá que examinar hasta qué punto disposiciones internas que establecen reglas diferentes

---

[69] STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536, apdo. 49.

[70] STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*. ECLI:EU:C:2024:536, apdos. 48 y 50.

[71] En el asunto *PS*, las normas supuestamente infringidas que daban lugar a compensación formaban parte de las regulaciones sobre la profesión de asesor fiscal.

de compensación de los daños en supuestos en los cuales hay un tratamiento de daños personales pueden llegar a menoscabar la efectividad del remedio indemnizatorio establecido en el Reglamento.

3.6. Pluralidad de sujetos responsables

La cadena de valor o ciclo de vida de la IA generativa implica diferentes estadios o tareas que pueden ser llevados a cabo por sujetos diferentes. No necesariamente el desarrollador de un modelo de IA generativa habrá elaborado él mismo las bases de datos utilizadas en su entrenamiento; puede encargar a un tercero que lleve a cabo tareas de *fine-tuning*; o puede licenciar el modelo a terceros para que sean estos quienes desarrollen sistemas o integren el modelo en sus propios servicios. La pluralidad de sujetos requerirá la identificación de los diferentes roles que hayan de corresponder a cada uno y el cumplimiento de los deberes establecidos en el RGPD para la distribución de responsabilidades. En particular, para cada operación de tratamiento o conjunto de tratamientos relacionados deberá examinarse qué sujeto o sujetos asumen la posición de responsable o corresponsables; y, en su caso, si otros actúan como encargados del tratamiento. La delimitación de las diferentes posiciones no siempre es sencilla, especialmente, por el concepto de corresponsabilidad en el tratamiento de datos personales que ha desarrollado el TJUE[72].

El artículo 26.1. RGPD señala que *«cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento […]»*. Para que haya corresponsabilidad, los diferentes sujetos han de poder ser considerados a título individual responsables del tratamiento *ex* artículo 4.7 RGPD, esto es, ambos han de haber influido efectivamente en la determinación de los fines y medios del tratamiento. Y, por otro lado, han de tener alguna relación entre ellos, puesto que su influencia en la determinación de los fines y medios debe ejercerse conjuntamente[73].

---

[72] En este sentido, véanse STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH /Facebook Ireland Ltd/Vertreter des Bundesinteresses beim Bundesverwaltungsgericht.* ECLI:EU:C:2018:388; STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyskunta.* ECLI:EU:C:2018:551; STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.* ECLI:EU:C:2019:629; y STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcijak.* ECLI:EU:C:2023:949.

[73] Sobre los diferentes criterios exigidos, véase Rubí Puig, A. (2024). El principio de culpabilidad en el derecho de protección de datos personales y la condición de responsable del tratamiento. *La* Ley *Unión Europea*, 121, 1-16.

La participación conjunta en la determinación de los fines y medios que genera la situación de corresponsabilidad en el tratamiento puede llevarse a cabo de maneras diversas: (i) un acuerdo o decisión común por dos o más personas; o (ii) una convergencia en las decisiones efectuadas independientemente, que se complementan para influir decisivamente en la determinación de los fines y medios. Sea como sea, no es necesario un acuerdo formal entre los implicados en las operaciones de tratamiento de datos personales para que surja una situación de corresponsabilidad. El TJUE patrocina una visión funcional y no formalista del derecho de protección de datos personales, que implica la necesidad de evaluar todas las circunstancias fácticas de cada caso para la asignación de roles y distribuciones de responsabilidades.

El TJUE ha resuelto que una situación de corresponsabilidad no exige una responsabilidad equivalente. Los diferentes corresponsables pueden estar implicados en diferentes etapas del tratamiento de los datos personales, pueden participar en diferentes grados o pueden obtener resultados diversos[74]. El TJUE también ha venido afirmado que, para darse una situación de corresponsabilidad, no es necesario que todos los corresponsables tengan acceso a los datos personales tratados[75].

Desde el punto de vista de la reparación de los daños, el artículo 82 RGPD también establece una serie de reglas que podrán jugar un papel importante en los pleitos contra diferentes agentes en la cadena de valor de la IA generativa, como potenciales responsables civiles.

En primer lugar, se establece una regla de solidaridad en el artículo 82.4 RGPD. Así, en caso de pluralidad de corresponsables, en supuestos de concurrencia de un responsable y un encargado del tratamiento o en otras situaciones de pluralidad subjetiva, *«cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado»*[76]. En segundo lugar, en la relación interna de solidaridad se prevé

---

[74] Véase Comité Europeo de Protección de Datos (7 de julio de 2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*. https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf, pp. 22-23.

[75] Véase, especialmente, STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629.

[76] Con arreglo al considerando 146 RGPD, un legislador interno puede decidir prescindir del carácter solidario de la obligación de reparar los daños y transformarla en una regla parciaria, siempre que se salvaguarde el derecho del interesado a recibir una indemnización total y efectivo. El legislador español ha optado por una regla de solidaridad. En este sentido, véase artículo 30.2. de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE nú,. 294 de 6.12.2018): *«Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados»*.

una acción de repetición o regreso para aquel demandado que haya satisfecho la indemnización total al perjudicado. Conforme al artículo 82.5 RGPD, este podrá *«reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados»*. De seguro, la implicación de varios agentes en la cadena de valor de la IA generativa va a ofrecer un buen campo de pruebas para examinar el funcionamiento de estas reglas en los futuros pleitos de responsabilidad civil por infracciones normativas del derecho de protección de datos personales.

4. CONCLUSIONES

El desarrollo y funcionamiento de modelos y sistemas de IA generativa conllevarán con frecuencia tratamientos de datos personales y, en efecto, incumbirá a sus desarrolladores y operadores cumplir con los principios y obligaciones establecidas en el RGPD y demás normativa protectora del derecho a la protección de los datos de carácter personal. En estos momentos, son muchas las cuestiones abiertas acerca de cómo ha de cumplirse con lo establecido en el RGPD –por ejemplo, hay dudas acerca de las bases de licitud que puedan amparar la compilación de bases de datos o el entrenamiento de modelos de IA generativa; acerca del nivel de medidas técnicas y organizativas exigibles; o acerca de la relación entre diferentes agentes en la cadena de valor de la IA generativa. Los rasgos generales de la IA generativa –gran tamaño, generalidad y opacidad– contribuyen a este nivel de incertidumbre, pero es esperable que en los próximos años agencias de protección de datos y tribunales vayan de modo progresivo ofreciendo respuestas y consolidando un marco legal de aplicación a los tratamientos de datos personales realizados en este ámbito. A pesar de la incertidumbre actual o acaso a consecuencia suya, es probable que algunos desarrolladores y operadores en la cadena de valor de la IA generativa hayan infringido ya o lleguen a infringir disposiciones del RGPD y, a resultas, hayan causado o causen daños y perjuicios a personas físicas.

Es probable también que algunas de estas personas entablarán acciones de responsabilidad civil para resarcirse de los daños sufridos como consecuencia del desarrollo y funcionamiento de herramientas de IA generativa. Cuando los daños y perjuicios sean de los que el RGPD persigue prevenir y compensar, el artículo 82 RGPD ofrecerá un buen fundamento para la responsabilidad civil de responsables y encargados de los tratamientos de datos personales en la cadena de valor de la IA generativa. Los litigios que se lleguen a plantear en este sector ofrecerán un campo de pruebas para examinar si la jurisprudencia

elaborada por el TJUE en interpretación de este precepto es adecuada o no para la IA generativa. Es probable que, en estos asuntos, se lleguen a examinar los problemas que han sido apuntados en este trabajo, tales como las consecuencias de reparar daños de bagatela y de fijar indemnizaciones simbólicas; la indemnizabilidad del temor a que los datos personales propios puedan ser utilizados ilícitamente en el futuro; la imputación subjetiva y objetiva de los daños derivados de incidencias en la seguridad de la información de modelos y sistemas de IA generativa; la compatibilidad del remedio previsto en el artículo 82 RGPD con otros fundamentos de responsabilidad civil; y la adecuación de una regla de solidaridad en la obligación de responder de varios sujetos implicados en la cadena de valor de la IA generativa.

BIBLIOGRAFÍA UTILIZADA

A) Literatura académica

Achille, A., Kearns, M., Klingenberg, C., y Soatto, S.0. (2023). AI model disgorgement: Methods and choices. *Proceedings of the National Academy of Sciences of the United States of America, 121* (https://doi.org/10.48550/arXiv.2304.03545).

Arroyo i Amayuelas, E. (2024). El scoring de Schufa. *InDret* 3.2024. 134-160.

Beckers, A., y Teubner, G. (2021). *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds*. Hart, 161-162.

Brown, H., Lee, K., Mireshghallah, F., Shokri, R., y Tramèr, F. (2022). What Does It Mean for a Language Model to Preserve Privacy?. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 2280–92. https://doi.org/10.1145/3531146.3534642.

Carlini, N., Tramer, F., Wallace, E., Jagielski, M. et al. (2021). Extracting Training Data from Large Language Models. *30th USENIX Security Symposium*. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting. 2633-2650.

Carlini, N., Hayes, J., Nasr, M., Jagielski, M., Sehwag, V., Tramèr, F., Balle, B., Ippolito, D., y Wallace, E. (2023). Extracting Training Data from Diffusion Models. *ArXiv, abs/2301.13188*.

Carrasco Perera, A. (Septiembre de 2024). El daño que consiste en no saber si se ha producido o no una infracción y un perjuicio de datos personales. *GA-P Análisis*. https://ga-p.com/publicaciones/el-dano-que-consiste-en-no-saber-si-se-ha-producido-o-no-una-infraccion-y-un-perjuicio-de-datos-personales/.

Carrière-Swallow,Y., y Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective. *IMF Departmental Papers* 19 (16), 2019. 1-46.

Chang, C. (2024). When AI Remembers Too Much: Reinventing The Right To Be Forgotten For The Generative Age. *Washington Journal of Law and Technology and the Arts, 19*(3) 22-45.

Chiara, P.G. (2023). Italy: Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing. *European Data Protection Law Review.*Vol. 9. 68–72.

Davara Rodríguez, M.A. (2021). Tratamiento (Comentario al Artículo4.2 RGPD). Troncoso Reigada A. (Dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Thomson Reuters –Civitas. 591-628.

El-Mhamdi, E., Farhadkhani, S., Guerraoui, R., Gupta, N., Hoang, L.N., Pinot, R., y Stephan, J. (2022). On the Impossible Safety of Large AI Models. *ArXiv, abs/2209.15259.*

Famularo, J. (2023). Platform-Related Harms., *Yale-Wikimedia Initiative on Intermediaries & Information*, 1-14. https://law.yale.edu/sites/default/files/area/center/isp/documents/platformrelatedharms_ispessayseries_2023.pdf. Págs. 8-9.

Gil González, E. (2022). *El interés legítimo en tratamientos de datos personales.* La Ley.

Guadamuz, A. (2024). A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs. *GRUR International, 73*(2), 111-127.

Gupta, M., Akiri, C., Aryal, K., Parker, E., y Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access, 11*, 80218-80245.

Hacker, P. (2021). A legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology, 13*(2), 257–301. https://doi.org/10.1080/17579961.2021.1977219.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., y Liang, P. (2023). Foundation Models and Fair Use. *Stanford Law and Economics Olin Working Paper* No. 584. https://ssrn.com/abstract=4404340.

Hine, E., Novelli, C., Taddeo, M., y Floridi, L. (2023). Supporting Trustworthy AI Through Machine Unlearning. *SSRN Scholarly Paper.* https://doi.org/10.2139/ssrn.4643518.

Kretschmer, M., Margoni, T. y Oruç, P. (2024). Copyright Law and the Lifecycle of Machine Learning Models. *IIC.* vol. 55. 110-138.

Lee, K., Cooper, F., y Grimmelmann, J. (2024). Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain. *Journal of the Copyright Society*, 2024. 1-128 (en prensa) (disponible a http://dx.doi.org/10.2139/ssrn.4523551).

Marcos, H., y Pullin, M. (Octubre 2023). Large Language Models and EU Data Protection: Mapping (Some) of the Problems. *The Digital Constitutionalist.* ht-

tps://digi-con.org/large-language-models-and-eu-data-protection-mapping-some-of-the-problems.

Martín Faba, J. M. (2024). Novedades en materia de indemnización y protección de datos personales. *Revista CESCO De Derecho De Consumo*, (49), 131–147. https://doi.org/10.18239/RCDC_2024.49.3474.

Moreno Martínez, J.A. (2021). El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores. Ataz López, J. y Cobacho Gómez, J.A. (Coords.) (2021). *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*. Thomson -Aranzadi, Tomo 3, 515-565.

Mühlhoff, R., y Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology*, *16*(1), 261–292. https://doi.org/10.1080/17579961.2024.2313794.

Necati Pehlivan, C. (19 de septiembre de 2024). Inteligencia artificial y protección de datos. *Almacén de Derecho.* https://almacendederecho.org/inteligencia-artificial-y-proteccion-de-datos.

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., y Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *ArXiv, abs/2401.07348*. 1-36.

Nunez Duffourc, M., Gerke, S., y Kollnig, K. (2024). Privacy of Personal Data In The Generative AI Data Lifecycle. *New York University Journal of Intellectual Property And Entertainment Law*. Vol. 13, n. 2. 219-268.

Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, 5(4), 53-87.

Rubí Puig, A. (2019). Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español. *Derecho Privado y Constitución*, 34, 197-232.

Rubí Puig, A. (2024). El principio de culpabilidad en el derecho de protección de datos personales y la condición de responsable del tratamiento. *La* Ley *Unión Europea*, 121, 1-16.

Rubí Puig, A. (2024). Inteligencia artificial y daños indemnizables. Álvarez Lata, N. (2024). *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial.* APPDC-Aranzadi. 621-688.

Ruschemeier, H. (2024). Generative AI and Data Protection. Calo, R., Ebers, M., Poncibò, C., y Zou, M. (2024). *Handbook on Generative AI and the Law*, Cambridge University Press (en prensa) (disponible en SSRN: https://ssrn.com/abstract=4814999).

Staab, R., Vero, M., Balunović, M. y Vechev, M. (2023). Beyond Memorization: Violating Privacy Via Inference with Large Language Models. https://arxiv.org/ abs/2310.07298.

Varoquaux, G., Luccioni, A.S., y Whittaker, M. (2024). Hype, Sustainability, and the Price of the Bigger-is-Better Paradigm in AI. (https://doi.org/10.48550/arXiv.2409.14160).

Zanfir-Fortuna, G. (12 de septiembre de 2023). How Data Protection Authorities are De Facto Regulating Generative AI. *Future of Privacy Forum*. https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/.

B) Guías e informes

AEPD (febrero de 2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf.

Bundesamtes für Sicherheit in der Informationstechnik (Abril de 2024). Generative AI Models Opportunities and Risks for Industry and Authorities. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4.

CNIL, "Les fiches pratiques sur l'IA", 2024 (https://www.cnil.fr/fr/les-fiches-pratiques-ia).

Comité Europeo de Protección de Datos (7 de julio de 2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*. https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf.

Confederation of European Data Protection Organisations (16 de octubre de 2023). Generative AI: The Data Protection Implications. *CEDPO AI Working Group*. https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf.

European Data Protection Supervisor (3 de junio de 2024). Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems. https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf.

Garante per la Protezione dei Dati Personali (septiembre de 2023). Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale. https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+ la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0.

Hamburg Commissioner for Data Protection and freedom of information (2024). Discussion Paper: Large Language Models and Personal Data. https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf.

JURISPRUDENCIA DEL TJUE

STJUE de 19 de octubre de 2016, asunto C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*. ECLI:EU:C:2016:779.

STJUE de 20 de diciembre de 2017, asunto C-434/16, *Peter Nowak c. Data Protection Commissioner*. ECLI:EU:C:2017:994.

STJUE de 5 de junio de 2018, asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH / Facebook Ireland Ltd/Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*. ECLI:EU:C:2018:388.

STJUE de 10 de julio de 2018, asunto C-25/17, *Tietosuojavaltuutettu c. Jehovan todistajat - uskonnollinen yhdyskunta*. ECLI:EU:C:2018:551.

STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV/Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*. ECLI:EU:C:2019:629.

STJUE de 24 de septiembre de 2019, asunto C-136/17, *GC y otros c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773.

STJUE de 17 de junio de 2021, asunto C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, ECLI:EU:C:2021:492.

STJUE de 24 febrero 2022, asunto C-175/20, *SS SIA c. Valsts ieņēmumu dienests*. ECLI:EU:C:2022:124.

STJUE de 1 de agosto de 2022, asunto C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601.

STJUE de 8 de diciembre de 2022, asunto C-180/21, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*. ECLI:EU:C:2022:967.

STJUE de 4 de mayo de 2023, asunto C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370.

STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. y otros c. Bundeskartellamt* (Condiciones generales del servicio de una red social), ECLI:EU:C:2023:537.

STJUE de 9 de noviembre de 2023, asunto C-319/22, *Gesamtverband Autoteile-Handel eV c. Scania CV AB*. ECLI:EU:C:2023:837.

STJUE de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcijak*. ECLI:EU:C:2023:949.

STJUE de 7 de diciembre de 2023, asunto C-634/21, *OQ c. Land Hessen y SCHUFA Holding AG*. ECLI:EU:C:2023:957.

STJUE de 14 de diciembre de 2023, asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986.

STJUE de 14 de diciembre de 2023, asunto C-456/22, *VX, AT c. Gemeinde Ummendorf*, ECLI:EU:C:2023:988.

STJUE de 25 de enero de 2024, asunto C-687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72.

STJUE de 7 de marzo de 2024, asunto C-604/22, *IAB Europe c. Gegevensbeschermingsautoriteit*. ECLI:EU:C:2024:214.

STJUE de 11 de abril de 2024, asunto C-741/21, *GP c. juris GmbH*, ECLI:EU:C:2024:288.

STJUE de 20 de junio de 2024, asuntos acumulados C-182/22 y C-189/22, *JU y SO c. Scalable Capital GmbH*, ECLI:EU:C:2024:531.

STJUE de 20 de junio de 2024, asunto C-590/22, *AT y BT contra PS GbR y otros*, ECLI:EU:C:2024:536.

STJUE de 12 de septiembre de 2024, asuntos acumulados C-17/22 y C-18/22, *HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG c. Müller Rechtsanwaltsgesellschaft mbH y otros*, ECLI:EU:C:2024:738.

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

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

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

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

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

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

9 788410 707085