REVISTA JUSTICIA & DERECHO
Universidad Autónoma de Chile
Volumen 8
Número temático 2025

UNIVERSIDAD AUTÓNOMA DE CHILE
MÁS UNIVERSIDAD

Recibido el 30 de julio de 2025 / Aprobado el 10 de noviembre de 2025
Article
doi: 10.32457/rjyd.v8it.3232

Retos jurídicos del tratamiento de los datos (personales y no personales) a través de sistemas de Inteligencia Artificial en el Derecho de la Unión Europea

Legal challenges of processing of (personal and non-personal) data through Artificial Intelligence systems within the European Union Law

Roberto Cippitani[1]

RESUMEN

El Reglamento (UE) 2024/1689 de la Unión Europea (el Artificial Intelligence Act "AI Act" en el acrónimo inglés) y otras fuentes destacan la importancia de los datos para los sistemas de inteligencia artificial ("IA"): de hecho, la IA funciona con datos personales y no personales en la entrada y, por otro lado, produce datos en la salida.

El objetivo de este artículo es identificar los principales problemas jurídicos derivados del uso de datos personales y no personales por parte de los sistemas de IA en el marco de la legislación de la Unión Europea.

En el caso de los datos personales, el AI Act establece la obligación de cumplir con el Reglamento General de Protección de Datos (GDPR) y otras normativas europeas. Respecto a los datos no personales, el AI Act reconoce intereses legales relacionados con la propiedad intelectual, los secretos comerciales, la seguridad pública y la confidencialidad.

Sin embargo, el uso masivo de datos en la IA puede dificultar los principios del GDPR (como la minimización o el consentimiento) y la tutela de los demás intereses.

[1] Codirector de la Cátedra ISAAC (Individual Rights, Scientific Research and Cooperation) de la Universidad Nacional de Educación a Distancia (UNED); profesor titular y presidente del Comité Académico, Maestría Derecho Judicial, Escuela Judicial del Poder Judicial del Estado de Oaxaca (México) y de INDEPAC - Instituto de Estudios Superiores en Derecho Penal (México); Investigador asociado del Consiglio Nazionale delle Ricerche (Italia), CNR-IFAC. El presente trabajo es el resultado de las actividades realizadas en el ámbito de los siguientes proyectos: Módulo Jean Monnet e-Ride "Ethics and Research Integrity in the Digital Age" (2024-2027), no. 101175756; Módulo Jean Monnet "Artificial Intelligence and European Private Law" (2023-2026); Cátedra Jean Monnet de Gobernanza y Regulación en la Era Digital (GovReDig)- no. 101127331. Email: roberto.cippitani@unipg.it

Desde el punto de vista ético-jurídico, el tratamiento de datos por las tecnologías plantea muchas cuestiones que solo parcialmente se pueden solucionar con normas específicas como el AI Act, el GDPR y otras normativas, que tienen enfoques y objetivos distintos.

Se deben identificar principios y reglas comunes, como la responsabilidad y la ética por diseño, que pueden generar sinergias e impulsar soluciones más eficientes y sostenibles.

Palabras claves: Inteligencia Artificial, datos personales, datos no personales, calidad de los datos, derechos humanos.

ABSTRACT

Regulation (EU) 2024/1689 (the Artificial Intelligence Act, or 'AI Act') and other European regulations emphasise the importance of data for the functioning of artificial intelligence (AI) systems. These systems use personal and non-personal data as input and generate data as output.

This article analyses the main legal issues that arise from the use of data by AI systems within the framework of European Union law.

With regard to personal data, the AI Act requires compliance with the General Data Protection Regulation (GDPR) and other applicable regulations without undermining the protection of fundamental rights. However, the large-scale processing of data in AI can put essential GDPR principles such as minimisation, purpose limitation and storage under strain, making it difficult to update and improve models. Likewise, obtaining informed consent can be problematic given the unpredictability and transformability of data.

Regarding non-personal data, the AI Act recognises legitimate interests relating to intellectual property, trade secrets, and public security. It therefore establishes governance practices to ensure data quality and traceability, supported by regulatory and interpretative strategies from European and national authorities.

Nevertheless, the ethical and legal challenges of AI-driven data processing cannot be fully resolved through sectoral regulations alone. Common principles, such as responsibility and ethics by design, are needed to promote technologies that align with European values while simultaneously protecting individual rights and collective interests.

Keywords: Artificial Intelligence, personal data, non-personal data, quality, human rights.

1. Inteligencia artificial y datos

El Reglamento (UE) 2024/1689 de la Unión Europea (el Artificial Intelligence Act, en adelante "AI Act" utilizando el acrónimo en inglés) [2] define un "sistema de IA" como una máquina diseñada:

> para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales (artículo 3.1 AI Act).

Además, según los documentos institucionales, la inteligencia artificial manifiesta un "comportamiento inteligente" al "(…) ser capaz, entre otras cosas, de recopilar y tratar datos, analizar e interpretar su entorno y pasar a la acción, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos".[3]

[2] 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.

[3] Vid. el artículo 4.a de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías (2020/2012(INL))

Los sistemas de este tipo realizan la "percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido" [4] esto ocurre mediante "varios enfoques y técnicas, como el aprendizaje automático (del que el aprendizaje profundo y el aprendizaje por refuerzo constituyen algunos ejemplos), el razonamiento automático (que incluye la planificación, programación, representación y razonamiento de conocimientos, búsqueda y optimización) y la robótica (que incluye el control, la percepción, sensores y accionadores así como la integración de todas las demás técnicas en sistemas ciberfísicos)". [5]

En el ámbito de la definición de la inteligencia artificial se identifican los "modelos de IA de uso general", es decir modelos entrenados con un gran volumen de datos utilizando autosupervisión a gran escala, que presentan un grado considerable de generalidad, capaces de realizar "una gran variedad de tareas distintas" (artículo 3, apartado 1, no. 62, AI Act).

Por lo tanto, el AI Act y otras fuentes destacan que los sistemas de IA utilizan datos de entrada y generan datos y otros productos derivados de la elaboración de las informaciones.[6]

Vista la relevancia de los datos en la disciplina europea sobre la materia, el objetivo del presente artículo es identificar los principales problemas jurídicos surgidos del uso de los datos, tanto personales como no personales por parte de los sistemas de inteligencia artificial, en el marco de la legislación de la Unión Europea.

Eso teniendo en consideración, como destaca el AI Act (Sarra, 2025), la compleja y multifacética legislación de la Unión sobre los datos personales, en particular, veáse a este respecto lo señalado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante "GDPR" desde el acrónimo en inglés por "General Data Protection Regulation" y otras normas[7]) y también atendiendo a la regulación vigente sobre los datos no personales.[8]

---

4 Grupo de expertos de alto nivel sobre IA en sus Directrices éticas para una inteligencia artificial confiable (2019). Disponible en: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60656

5 Ibidem.

6 Los datos en las fuentes del Derecho UE se definen como "toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual" (véase el artículo 2, no. 1, Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)).

7 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas); Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

8 Entre las fuentes jurídicas que se refieren a los datos vid: El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 ("Data Act"); el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 ("Data Governance Act"); la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, y otros textos normativos, entre los cuales sobre todo el AI Act. Además, hay que considerar la disciplina de los "Espacios europeos de datos", prevista en la Comunicación "Estrategia europea de datos".
Un Espacio europeo de datos es (vid. el "considerando" 2 del Data Governance Act).:

2. IA y datos personales

2.1. AI Act y protección de datos personales

El AI Act se centra especialmente en el uso de los datos personales. En efecto, el artículo 2, apartado 7, del AI Act prescribe que:

> el Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento.

Especialmente, se establece que el reglamento no debe afectar al GDPR y a las otras normas de la Unión en materia de protección de datos personales.

El "considerando" 10 del reglamento comentado contiene un resumen de las consecuencias de su aplicación conjunta con el GDPR (además de con otras normas): la disciplina de protección de datos personales se debe aplicar a los conjuntos de datos utilizados por la inteligencia artificial, sean datos personales o no personales; el AI Act no afecta las funciones y competencias de las autoridades de supervisión independientes competentes en materia de protección de datos personales; deberán ser respetadas las obligaciones de los proveedores y los responsables del despliegue de sistemas de inteligencia artificial como responsables o encargados del tratamiento de datos; las personas interesadas siguen disfrutando de todos los derechos y garantías que les confiere dicho Derecho de la Unión, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles; las normas del reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados para proteger los datos personales y otros derechos fundamentales.

Asimismo, el respeto de los derechos asociados a los datos personales se debe garantizar a lo largo de todo el ciclo de vida del sistema de inteligencia artificial ("considerando" 69 AI Act), aplicando los principios previstos por el GDPR (vid. especialmente el artículo 5 GDPR) como el de minimización, así como el principio de protección de datos desde el diseño y por defecto (vid. artículo 25 GPDR). Para ello, los responsables y encargados del tratamiento de los datos deberán utilizar la anonimización y el cifrado ("considerando" 69).[9]

2.2 Aspectos críticos en el uso de datos personales por los sistemas se IA

Sin embargo, la aplicación conjunta de la disciplina de protección de datos personales y de la AI Act podrán dar origen a algunos asuntos problemáticos. En ese sentido, en primer lugar, puede ser difícil garantizar la aplicación de los principios previstos por el GDPR (vid. en particular el artículo 5) y por otras fuentes. De hecho, el uso masivo de datos, típicos de las tecnologías actuales usadas en la inteligencia artificial, puede

un mercado interior de datos en el que estos pudieran utilizarse independientemente de su ubicación física de almacenamiento en la Unión de conformidad con el Derecho aplicable, lo que, entre otras cosas, podría resultar fundamental para el rápido desarrollo de las tecnologías de inteligencia artificial.

Se prevé la adopción de unas fuentes jurídicas que reglarán los espacios europeos de datos en diferentes ámbitos. El primer reglamento aprobado has sido Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo de 11 de febrero de 2025 relativo al Espacio Europeo de Datos de Salud.

[9] También el Consejo de Europa (Guidelines on Artificial Intelligence and data protection, 25 de enero 2019, puntos 8 sigs.) plantea la necesidad de garantizar los derechos de las personas interesadas a no ser objeto de una decisión que les afecte significativamente basada únicamente en un tratamiento automatizado; la libertad de elección de los usuarios sobre el uso de la IA, ofreciendo alternativas viables a las aplicaciones de IA; el derecho de oposición en relación con el tratamiento basado en tecnologías que influyen en las opiniones y el desarrollo personal de los individuos; entre otros.

constituir un obstáculo a los principios de minimización (Finck & Biega, 2021), exactitud (Novelli et al., 2024), limitación y finalidad[10] y también pueden restringir la capacidad de almacenamiento (Mitrou, 2018; Artzt & Viet Dung, 2022).

Como se sabe, las limitaciones de almacenamiento restringen el tiempo durante el que se pueden conservar los datos personales y la frecuencia con la que se pueden reutilizar o actualizar los modelos utilizando los datos personales originales. Esta limitante hace difícil mejorar los modelos de IA, ya que es posible que un proveedor (u otro operador) de sistemas de inteligencia artificial no pueda conservar o reutilizar los datos para el reentrenamiento o la actualización de los modelos, lo que podría reducir la innovación y la adaptabilidad.

Además, la naturaleza de "caja negra" de muchos modelos de inteligencia artificial de alto rendimiento dificulta ofrecer las explicaciones significativas y la transparencia exigida por el GDPR (Sacramed, 2024).

La jurisprudencia en temas de algoritmos e inteligencia artificial ha afirmado la necesidad de que los datos y otros elementos sean trasparentes, especialmente para permitir la defensa de los derechos y los intereses que se plantean por decisión de una administración pública (vid. en particular la determinación del *Conseil Consitutional* francés,[11] del *Consiglio di Stato* italiano,[12] pero también la sentencia en el asunto Syri[13]).

Las dificultades técnicas se refieren a que la manera de funcionar de los sistemas de inteligencia artificial muchas veces no es expresable en términos humanos (Reed, 2018) e implican algún elemento aleatorio que produce resultados no reproductibles por diseño (Ishii, 2019). Por el contrario, algunos autores opinan que la *explicabilidad* de la inteligencia artificial y de su proceso de toma de decisiones no puede excluirse de ninguna manera, pues ya existen investigaciones sobre el tema de la interpretabilidad de la IA (Miron, 2008).

En segundo lugar, puede ser complicado probar que sean respetados derechos específicos como el consentimiento informado o el derecho a la cancelación.

Sobre el primero de estos puntos, el consentimiento informado de la persona interesada, este se presenta como "irreal y menos significativo" ya que depende del carácter mutable de los datos tratados y a la imprevisibilidad de los resultados del tratamiento. La complejidad y el uso transformador de los macrodatos no ofrecen a los interesados la posibilidad real de comprender los posibles usos futuros para poder elegir conscientemente.[14] Como ha afirmado el Supervisor Europeo de Protección de Datos, *"we may not have the appropriate information about how our personal data is used and importantly, how decisions concerning us are taken, therefore making it impossible to meaningfully consent to the use (processing) of our data*" ("Es posible que no dispongamos de la información adecuada sobre cómo se utilizan nuestros datos personales y, lo que es más importante, cómo se toman las decisiones que nos afectan, lo que nos impide dar nuestro consentimiento de forma significativa al uso (tratamiento) de nuestros datos") (Buttarelli, 2016).

---

10 Esto podría incluir el tratamiento de datos con fines hipotéticos que no se hayan determinado previamente. El principio de limitación de la finalidad no puede ajustarse plenamente, ya que los nuevos fines del tratamiento de datos pueden considerarse inesperados o inadecuados (Artzt & Viet Dung, 2022, p. 52).

11 Conseil Constitutionnel, sentencia nº2018-765 del 12 de junio de 2018, en https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm.

12 Consiglio di Stato, sent. 4 de abril de 2019, n.º 2270; Consiglio di Stato, sent. 13 de diciembre de 2021, n.º 8472.

13 Tribunal de Distrito de La Haya (Países Bajos), 5 de febrero de 2020.

14 Mitrou, 2018; vid. también las críticas a la aplicación formal y matemática del GDPR, y especialmente del consentimiento, por las BighTech, F. van Daalen et. al., 2025.

Sobre el segundo de los puntos mencionados, el derecho de cancelación, ciertamente otro desafío se refiere al consentimiento. El derecho a retirarlo refleja y garantiza el derecho de la persona a la autodeterminación informativa, y los responsables del tratamiento de datos deben crear la capacidad técnica necesaria para satisfacer las solicitudes de los interesados de retirar su consentimiento. Sin embargo, esta acción

y, respectivamente, la retirada/eliminación de datos tiene un impacto pues puede afectar el desarrollo de la inteligencia artificial porque limitaría la cantidad de datos disponibles para aprender (Mitrou, 2018, p. 40).

Debido a las dudas sobre la validez del consentimiento para el tratamiento de datos y a las dificultades asociadas con él en un contexto de macrodatos e inteligencia artificial, es probable que las organizaciones también deseen desarrollar una justificación basada en intereses legítimos para el tratamiento de la información.

El GDPR no se refiere al tratamiento de dicha información anónima, ni siquiera con fines estadísticos o de investigación. Sin embargo, el procesamiento de los *big data* por la inteligencia artificial lleva a identificar nuevas correlaciones entre los datos y (re)agruparlos o a crear nuevos tipos y categorías de ellos, a veces sin la previsión del responsable del tratamiento (Mantelero, 2014). En la literatura especializada se ofrece este ejemplo:

> *Although the artificial intelligence may not process the special category of data itself, it may inadvertently create a profile based on secondary data (for example post code, social media data and shopping habits) of which all the individuals matched by the profile are of the same race or share another special category of data*." ("Aunque la inteligencia artificial puede no tratar la categoría especial de datos en sí, puede crear inadvertidamente un perfil basado en datos secundarios (por ejemplo, código postal, datos de redes sociales y hábitos de compra) donde todas las personas con las que coincida el perfil sean de la misma raza o comparten otra categoría especial de datos") (Butterworth, 2018, p. 262).

Se ha demostrado que los modelos de inteligencia artificial generativa pueden revelar datos personales a través de la fuga de informaciones y la inversión de modelos (Novelli et al., 2024, p. 5).[15]

En general, las particularidades de las tecnologías de la inteligencia artificial —como la opacidad, la complejidad, la imprevisibilidad y un comportamiento parcialmente autónomo—, dificultan comprobar el cumplimiento de la legislación vigente sobre protección de derechos fundamentales. En efecto, en muchos casos los resultados de salida no se podrán prever, lo que no dependerá del diseño sino de la correlación de los datos.

3. IA y datos no personales

El AI Act releva otros intereses jurídicos asociados a los datos no personales, como por ejemplo, "los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales (…) los intereses de seguridad pública y nacional, la integridad de los procedimientos penales y administrativos y la integridad de la información clasificada" así como la confidencialidad (considerando

[15] Esta es la razón por la cual la Autoridad de supervisión irlandesa (Data Protection Commission) con la comunicación del 14 de junio de 2024 ha acogido con satisfacción la decisión de Meta de suspender sus planes de entrenar su gran modelo lingüístico utilizando contenidos públicos compartidos por adultos en Facebook e Instagram en toda la Unión Europea (https://www.dataprotection.ie/en/news-media/latest-news/dpcs-engagement-meta-ai).

167 y el artículo 78 AI Act). En particular, la inteligencia artificial no debe poner en peligro el interés individual y general a la seguridad (Cippitani, 2023).

Entre las informaciones peligrosas para la seguridad pueden considerarse las "informaciones clasificadas"[16] y las relativas a asuntos como[17]: explosivos; defensa CBRN (química, biológica, radiológica y nuclear); infraestructuras y servicios públicos críticos[18]; seguridad fronteriza; terrorismo; delincuencia organizada; espacio de seguridad digital; investigación espacial, etcétera. En general, se trata de informaciones que pueden utilizarse de manera indebida (*misuse* de las informaciones) (Mayta-Tovalino et al., 2024), es decir arriesgando derechos individuales e intereses fundamentales.

> Otro tema importante que los sistemas de inteligencia artificial deben tener en cuenta son los derechos de propiedad intelectual e industrial y los secretos comerciales. En particular, hay que considerar que: los modelos de IA de uso general (…) los grandes modelos de IA generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores respecto de la manera en que se crea, distribuye, utiliza y consume su contenido creativo ("considerando" 105 AI Act).

La IA utiliza y pone a disposición del público conjuntos de datos sin una información clara sobre las licencias o los derechos que terceros tienen sobre ellos. Esto genera incertidumbre entre los usuarios sobre la forma en que tales datos pueden o no utilizarse, lo que conduce a su reutilización ineficaz (Farrel, 2023, p. 41).

Por otro lado "los proveedores de modelos de IA de uso general deben adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir la reserva de derechos expresada por los titulares de derechos con arreglo al artículo 4, apartado 3, de la Directiva (UE) 2019/790" ("considerando" 106 AI Act).

Los grandes modelos lingüísticos se entrenan utilizando materiales en línea, a menudo contenido protegido por derechos de autor (Ruschemeier, 2025). El uso de sistemas de IA para la así llamada "minería de textos y datos" también plantea algunos problemas, particularmente en el contexto de la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital. Efectivamente, la directiva introduce una excepción a los derechos de autor para la minería de textos y datos con fines de investigación científica, pero también permite a los Estados miembros implementar excepciones para otros fines, como el uso comercial. Sin embargo, los titulares de derechos pueden reservarse el derecho a evitar la minería de textos y datos, exigiendo a los proveedores de modelos de IA que obtengan autorización para tales actividades. Sin embargo, la publicación de modelos de inteligencia artificial de propósito general bajo licencia libre y de código abierto no revela necesariamente información sustancial sobre el conjunto de datos utilizado para el entrenamiento o el ajuste del modelo y sobre cómo se garantizó el cumplimiento de la ley de derechos de autor.

---

[16] Según la Decisión (UE, Euratom) n°2015/444 de la Comisión del 13 de marzo de 2015 sobre las normas de seguridad para la protección de la información clasificada de la UE y en otras fuentes como la Decisión (UE, Euratom) n°2021/259 de la Comisión europea del 10 de febrero de 2021 en la que se establecen normas de desarrollo sobre la seguridad industrial en relación con las subvenciones clasificadas, deben ser consideradas clasificadas (artículo 3, apartado 1, Decisión 2015/444):

> toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios Estados miembros.

[17] "Guidelines on the classification of information in Horizon Europe projects", párr. 4.2 sigs.

[18] Vid. Directiva 2008/114/CE del Consejo del 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Otros problemas de coordinación con el AI Act se pueden imaginar con referencia a las fuentes jurídicas reguladoras n del sector digital (Digital Markect Act, Data Service Act, la Directiva 2019/1024, relativa a los datos abiertos y la reutilización de la información del sector público, consúltese la nota número 8). Por ejemplo, la protección del secreto industrial puede entrar en conflicto con el principio de trasparencia previsto por el AI Act[19], pero también con el principio de la libre circulación y de reutilización previstos por otras fuentes jurídicas; por otro lado, la libre circulación de datos y el acceso abierto previstos pueden encontrar obstáculos en la AI Act que impone restricciones basadas en el riesgo; el Data Act exige acceso justo, en cambio el AI Act promueve la transparencia, al mismo tiempo que demanda documentación y trazabilidad mucho más exigentes para determinados sistemas (por ejemplo, registro de *datasets* de entrenamiento), lo que puede colisionar con la confidencialidad comercial o con los límites del propio Data Act respecto a secretos empresariales. Otros posibles casos problemáticos podrían surgir del uso de la inteligencia artificial y de la aplicación de la disciplina de los espacios europeos de datos (vid. la nota 8), como el "Espacio Europeo de Datos de la Salud", en este orden de cosas, el Reglamento (UE) 2025/327 reconoce que "muchos conjuntos de datos no están armonizados, lo que plantea problemas de comparabilidad y dificulta la investigación transfronteriza" ("considerando" 87), lo que puede causar un riesgo que los datos reutilizados para la IA no tengan la calidad suficiente (completitud, validez, actualidad) para los fines previstos, lo que puede generar decisiones erróneas o sesgadas; igualmente, el artículo 61, apartado 3, del Reglamento 2025/327 prevé que "los usuarios de datos de salud no reidentificarán ni intentarán reidentificar a las personas físicas a que se refieran los datos de salud electrónicos obtenidos por los usuarios de datos de salud", pero ese resultado puede ser frustrado por el uso de la inteligencia artificial aplicada a los conjuntos de datos; en suma, podrán producirse problemas debido a la tensión entre la reutilización de datos por la IA y la protección de secretos industriales y derechos de propiedad (vid. el "considerando" 60 Reglamento (UE) 2025/327).

Además, todavía no está claro cuáles normas y principios deberán aplicarse al uso de la inteligencia artificial en ámbitos que quedan excluidos por el AI Act, como la investigación científica (vid. el "considerando" 25), lo mismo que en el caso de tratamiento de datos mediante la IA por parte de las fuerzas y cuerpos de seguridad[20]. Sin embargo, en la actualidad algunos de los problemas mencionados son atendidos normalmente por las autoridades supervisoras, pero solo de forma indirecta, en la medida que se refieren a datos personales.[21]

En definitiva, un apoyo más específico para enfrentar los problemas de coordinación entre normativas lo darán las autoridades previstas por el AI Act y la Comisión Europa, así como la jurisprudencia.

[19] Aunque dicho contraste no se pueda considererar automatico y en base solo a la perspectiva de las empresa, sino averiguado incluso a través de expertos independientes, vid. AEPD (Agencia Espanola de Protección de Datos), Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, en https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf, p. 34.

[20] Materias subjetas a normas como la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; y el Reglamento (UE) 2024/982 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, relativo a la búsqueda y al intercambio automatizados de datos para la cooperación policial, y por el que se modifican las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los Reglamentos (UE) 2018/1726, (UE) 2019/817 y (UE) 2019/818 del Parlamento Europeo y del Consejo (Reglamento Prüm II).

[21] Se trata de cuestiones destacadas por la medida adoptada por el Garante italiano de protección de datos personales del 31 de marzo de 2023, que suspendió por un periodo ChatGPT en Italia, plateando la violación de la disciplina del GDPR (falta de consentimiento, ausencia de un filtro para cerciorarse de la edad de los usuarios) y la supuesta amenaza a otros intereses como, por supuesto, el derecho de autor y la seguridad (vid. Cippitani & Castrogiovanni, 2023). Pero estas últimas cuestiones no fueron enfrentadas incluso en las medidas siguientes (Vid. Garante italiano, 2024a). Otro caso interesante es el posible contraste del tratamiento de datos personales para objetivos de seguridad e investigación científica: vid. (Garante italiano, 2024b).

Cabe recordar, que la Comisión europea —en base al artículo 56, apartado 4, AI Act— está adoptando un "Código de prácticas de IA de uso general". Los capítulos de este instrumento recién aprobados el 10 de julio de 2025 están dedicados, específicamente, a las obligaciones en materias de trasparencia, seguridad y derecho de autor.[22]

En síntesis, los capítulos del Código de prácticas prevén que se pongan en marcha acciones de evaluación del riesgo, medidas de mitigación y que se sujetarán los sistemas a una evaluación independiente (vid. capítulo concerniente la seguridad); también contemplan la elaboración de documentos actualizados y al mismo tiempo buscan el resguardo de los principios de integridad, confidencialidad y trazabilidad de los datos documentados (vid. el capítulo sobre la trasparencia); la construcción de una política de cumplimiento de *copyright* y de medidas para evitar la violación del derecho de autor (por ejemplo, usando solo contenidos legalmente accesibles y no infringir medidas tecnológicas como DRM); estableciendo canales para que los titulares de derechos puedan presentar reclamaciones (véase el capítulo sobre el *copyright*).

4. La IA y la obligación del respeto de los derechos fundamentales

Otra categoría de problemas, que puede referirse tanto a los datos personales como a los no personales, es que el tratamiento de datos mediante sistemas de IA puede "dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos (…) generar riesgos y menoscabar los intereses públicos y derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible e incluye los perjuicios físicos, psíquicos, sociales o económicos." ("considerando" 5 AI Act).

Obviamente, entre los derechos fundamentales que hay que proteger, el AI Act confirma la naturaleza de derecho fundamental de la protección de los datos personales (artículo 8 de la Carta UE y el artículo 16 TFUE) (Sobre la protección de datos personales como derecho fundamental, vid. Irion, 2016). Pero la cuestión de la tutela de los derechos fundamentales en el uso de los datos es más amplia que la privacidad.

La comunicación "Generar confianza en la inteligencia artificial centrada en el ser humano" (párr. 2.2.v) recuerda que la toma de decisiones asistida por inteligencia artificial puede provocar discriminaciones. En esta línea, establece que:

> Los conjuntos de datos utilizados por los sistemas de IA (tanto para el entrenamiento como para el funcionamiento) pueden verse afectados por la inclusión de sesgos históricos involuntarios, por no estar completos o por modelos de gobernanza deficientes. La persistencia en estos sesgos podría dar lugar a una discriminación (in)directa. También pueden producirse daños por la explotación intencionada de sesgos (del consumidor) o por una competencia desleal. Por otra parte, la forma en la que se desarrollan los sistemas de IA (por ejemplo, la forma en que está escrito el código de programación de un algoritmo) también puede estar sesgada.

Así, la protección de los derechos fundamentales se muestra como importante en el sistema jurídico-ético de la UE, y especialmente en ámbito de las tecnologías (Benlloch Domènech & Sarrión Esteve, 2022).

[22] En https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai .

El uso de los datos debe respetar la "diversidad, no discriminación y equidad", lo que implica que los sistemas de inteligencia artificial se desarrollen y utilicen de un modo que incluya a diversos agentes y promueva la igualdad de acceso y de género, así como la diversidad cultural, al tiempo que se eviten los efectos discriminatorios prohibidos por el Derecho nacional o de la Unión. Para ello, deben evitarse sesgos injustos, puesto que los conjuntos de datos que utilicen los sistemas de inteligencia artificial pueden dar lugar a prejuicios y discriminación contra grupos o personas.[23] En consecuencia, siempre que sea posible, los sesgos identificables y discriminatorios deben eliminarse en la fase de recopilación de la información.

Para cumplir con lo anterior, un requisito se refiere a la necesidad de que las organizaciones que despliegan aplicaciones de IA sean conscientes de los efectos y las implicaciones que este despliegue puede tener sobre las personas y sus derechos y libertades, pero también sobre las comunidades y los grupos sociales.[24]

En lo que respecta a la imparcialidad, en la literatura se señala la importancia de considerar, a la hora de diseñar y desplegar procesos de aprendizaje automático, que tales procesos pueden estar "sesgados" para producir los resultados perseguidos por su diseñador (Kamarinou et al., 2016, p. 16). La autoridad francesa de protección de datos personales CNIL (*Commission nationale de l'informatique et des libertés*) señala acertadamente que todos los algoritmos están sesgados en cierto sentido, en la medida en que siempre son el reflejo de un conjunto de opciones y valores sociales, dependiendo de su configuración o los datos que se utilizan durante el entrenamiento. [25]

Otros problemas derivan de los riesgos de discriminación.[26] La injusticia puede surgir ya con la elección de los datos de formación. Al introducir un sesgo directo o indirecto en el proceso, la cantidad y la calidad de los datos utilizados para entrenar el algoritmo, incluida la fiabilidad de sus fuentes y etiquetado, pueden tener un impacto significativo en la construcción de perfiles, el reconocimiento de rostros o la detección de emociones. El sesgo puede introducirse en los procesos de aprendizaje automático en varias fases, como en el diseño del algoritmo y en la selección de los datos de entrenamiento, lo que puede incorporar prejuicios existentes en los procesos automatizados de toma de decisiones.

Entre las medidas que se deben adoptar para el respeto de los derechos humanos (Martínez, 2019), cabe destacar el rol de la evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo, prevista per el artículo 27 AI Act, análogamente al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680. Esta evaluación debe complementar la evaluación relativa a la protección de datos.[27]

[23] Vid. el art. 9 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas. En Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, cit.

[24] CNIL, Comment permettre à l'homme de garder la main ? - Les enjeux éthiques des algorithmes et de l'intelligence artificielle, 2017, p. 31.

[25] CNIL, Comment permettre à l'homme de garder la main ? - Les enjeux éthiques des algorithmes et de l'intelligence artificielle, cit.

[26] Ibidem. p. 31.

[27] El considerando 27 antemencionado hace referencia a las Directrices éticas para una IA digna de confianza, redactadas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisióny publicadas en el 2019. Vid. Comisión Europea, Grupo Independiente de expertos de alto nivel sobre Inteligencia Artificial, *Directrices éticas para una IA fiable*, 8 de abril de 2019, en https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

5. Gobernanza y calidad de los datos

Para evitar la violación de los derechos y de otros intereses fundamentales el AI Act se preocupa de "instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad" ("considerando" 67 AI Act). Del mismo modo, el artículo 26, apartado 1, establece que "Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen". Se trata de la afirmación del principio de *accountability* previsto en el uso de los sistemas de IA ("considerando" 27 AI Act)[28] y que está confirmado por el artículo 25 GDPR.

Sin embargo, la obligación más interesante respecto a los datos es la de garantizar su calidad. Se trata de un tema muy relevante y novedoso, ya que supone un cambio de paradigma respecto de ellos, y especialmente de los datos no personales. Con él, los datos dejan de considerarse como entidades sin valor y sin calidad. Además, la calidad de los datos se debe garantizar respetando los derechos de las personas y otros intereses anteriormente tratados.

No obstante, permanecen los problemas que han destacado en la búsqueda de un equilibrio entre el AI Act y otras normativas en materia de datos. Como se afirma en el considerando 67 (ver también al artículo 10, apartados 2 y 3):

> Los conjuntos de datos deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los colectivos de personas en relación con el uso de sistemas de IA de alto riesgo, prestando una atención especial a la mitigación de los posibles sesgos en los conjuntos de datos que puedan afectar a la salud y la seguridad de las personas físicas, tener repercusiones negativas en los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando los datos de salida influyan en la información de entrada de futuras operaciones (bucles de retroalimentación).

La cuestión de la calidad de los datos está planteada también por el "considerando" 71 GDPR que prevé que:

> el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error" y la posibilidad que el tratamiento sea discriminatorio.

Para desarrollar y evaluar sistemas de inteligencia artificial de alto riesgo con datos de calidad el AI Act (véase el considerando 68) tiene que acceder a los "espacios comunes europeos de datos" establecidos por la Comisión:

> Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a datos sanitarios y el entrenamiento, a partir de esos conjuntos de datos, de algoritmos de IA de una manera segura, oportuna, transparente, fiable y que respete la intimidad, y contando con la debida gobernanza institucional.

[28] Disponible en https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Según el artículo 17 apartado 1 del AI Act, los proveedores de sistemas de inteligencia artificial de alto riesgo establecerán un sistema de gestión de la calidad en que "se recojan las políticas, los procedimientos y las instrucciones":

> los sistemas y procedimientos de gestión de datos, lo que incluye su adquisición, recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con esa finalidad" (letra f).

Los criterios generales para construir sistemas de calidad están establecidos por el artículo 10 del AI Act, que prevé los conjuntos de datos de entrenamiento, validación y prueba deberán someterse a prácticas de gobernanza y gestión.

En particular, se deberá adoptar medidas para evitar, detectar, prevenir y mitigar:

> posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones (véase. artículo 10, apartado 2, f) e i) AI Act).

Será interesante comprobar en el próximo período, también a través del control jurisprudencial y de las autoridades administrativas, cómo se aplicarán estos criterios en la práctica y si realmente permitirán una gestión sostenible de los datos mediante la inteligencia artificial.

6. Calidad de los datos personales

Los organismos europeos competentes en materia de datos personales están tratando de aplicar las reglas y los principios previstos en el GDPR y otras fuentes al funcionamiento de los sistemas de inteligencia artificial.

Con tal propósito, el Consejo de Europa en su *Guidelines on Artificial Intelligence and data protection*, 25 de enero 2019 recomienda (punto 4) evaluar de forma crítica la calidad, la naturaleza, el origen y la cantidad de datos personales utilizados, reduciendo los datos innecesarios, redundantes o marginales durante las fases de desarrollo y entrenamiento, y supervisando después la precisión del modelo a medida que se alimenta con nuevos datos y el uso de datos sintéticos[29] para minimizar la cantidad de datos personales procesados por las aplicaciones de inteligencia artificial.

En particular se debe tener en cuenta el riesgo de que los datos y los modelos algorítmicos descontextualizados tengan repercusiones negativas sobre las personas y la sociedad.

[29] Los datos sintéticos se generan a partir de un modelo de datos construido sobre datos reales. Deben ser representativos de los datos reales originales. Véase la definición de datos sintéticos en OCDE. 'Glossary of Statistical Terms'. 2007. http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf

El Comité europeo de protección de datos personales (que reúne a las autoridades nacionales y europeas en materia de protección de datos personales) recuerda que si un sistema de inteligencia artificial usa datos personales eso implica un tratamiento y aplicación del GDPR[30]. Por otro lado, el Comité:

> considera que los modelos de IA entrenados con datos personales no pueden, en todos los casos, considerarse anónimos. En su lugar, la determinación de si un modelo de IA es anónimo debe evaluarse, sobre la base de criterios específicos, caso por caso.[31]

El Comité europeo afirma la necesidad de proteger los datos personales en cada fase de tratamiento,[32] especialmente en la colección de datos necesarios para el desarrollo y el entrenamiento de los sistemas.

Los organismos europeos no creen que el tratamiento de datos personales a través de la inteligencia artificial pueda constituir una excepción a la aplicación de los principios y reglas del GDPR. En particular el Supervisor europeo opina que es errónea la idea de que el principio de minimización de datos no tiene cabida en el contexto de la inteligencia artificial[33]. Sin embargo, los responsables del tratamiento de datos tienen la obligación de limitar la recogida y el tratamiento de datos personales a lo estrictamente necesario para los fines del tratamiento, evitando el uso indiscriminado de ellos. Porque la utilización de grandes volúmenes de datos para entrenar un sistema de IA generativa no implica necesariamente una mayor eficacia o mejores resultados.

Además, se deben implementar los otros principios y reglas, como la necesidad de identificar una de las bases jurídicas para el tratamiento (es decir, consentimiento, contrato, obligación legal, interés vital, interés público, interés legítimo), así como las previstas en el artículo 6 GDPR. Debido a las dificultades de conseguir el consentimiento, hay que demostrar, por ejemplo, el interés legítimo del responsable del tratamiento y que dicho interés tiene que existir antes del inicio del tratamiento de los datos.[34]

Como ejemplos de interés legítimo,[35] el Comité europeo cita: (i) desarrollar el servicio de un agente conversacional para ayudar a los usuarios; (ii) desarrollar un sistema de IA para detectar contenidos o comportamientos fraudulentos; y (iii) mejorar la detección de amenazas en un sistema de información.

El interés legítimo debe ser lícito, explicado en forma clara y precisa, y especialmente "real y presente, no especulativo".[36] Por lo tanto, dicho interés no se puede solo afirmar en abstracto sin concretamente demostrarlo (van Daalen, 2025, p. 32).

[30] (Comité europeo de proteción de datos personales, 2024a); vid. también la opinión del Supervisor europeo: European Data Protection Supervisor, Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems, 3 de junio de 2024, en https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en, párr. 3.

[31] (Comité europeo de proteción de datos personales, 2024b, párr. 34)

[32] (Comité europeo de proteción de datos personales, 2024a, párr. 14); European Data Protection Supervisor, Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems, op. cit., párr. 6.

[33] European Data Protection Supervisor, Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems, op. cit., párr. 7.

[34] Comité europeo de protección de datos personales, Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), GDPR en el contexto de la prestación de servicios en línea a los interesados, Versión 2.0, 8 de octubre de 2019, párr. 43. Vid. también Garante italiano, 2024b, esp. 3.2.1.

[35] (Comité europeo de proteción de datos personales, 2024, párr. 69)

[36] (Comité europeo de proteción de datos personales, 2024b, párr. 68)

En acuerdo con la jurisprudencia del Tribunal de Justicia de la Unión Europea,[37] una vez identificado el interés legítimo, se debe demostrar que el tratamiento debe ser necesario para alcanzar dicho interés,[38] y hay que realizar una ponderación que no supere los derechos del interesado[39] (el *balancing test,* previsto por el artículo 6, apartado 1, lit. f, GDPR) (Novelli et al., 2024, p. 5).

El Comité destaca que es fundamental garantizar la transparencia sobre el uso de datos en modelos de IA. Los interesados deben ser informados del uso de sus datos, y se les deben facilitar mecanismos para ejercer sus derechos de acceso, rectificación, oposición y supresión conforme al GDPR. Además, los responsables deben considerar las expectativas razonables del interesado al usar datos obtenidos de fuentes públicas o mediante *Web scraping*.[40]

En el dictamen 28/2024 el Comité propone la adopción de medidas para garantizar de manera proactiva la protección de los derechos de las personas interesadas[41], sea en la fase de desarrollo del modelo (por ejemplo, filtrado proactivo de datos personales antes del entrenamiento del modelo; análisis y eliminación de categorías especiales de datos;[42] aplicación de técnicas de anonimización o pseudonimización robustas y evaluables; diseño del modelo para evitar memorizar datos, etcétera) ya sea en la fase de despliegue del modelo (por ejemplo: implementación de filtros de salida (*output filters*) para detectar y bloquear respuestas que puedan contener datos personales; sistemas de supervisión humana; mecanismos de atención a los derechos del interesado; auditorías internas y externas periódicas sobre el comportamiento del modelo; etcétera).

Según los organismos europeos dichas medidas se deben adoptar *ex ante* y deben estar asociadas con una Evaluación de Impacto sobre la Protección de Datos (DPIA) cuando haya alto riesgo, y su efectividad debe poder demostrarse conforme al principio de rendición de cuentas (artículos 5.2 y 24 GDPR).

7. Conclusiones

La IA y otros importantes fenómenos científicos y tecnológicos de la presente época —entre los cuales se encuentran el *big data*, la genética (Cippitani, 2018), los biobancos (Colcelli et al., 2023), y las neurotecnologías (Cornejo-Plaza et al., 2024; Cornejo-Plaza, 2021) — utilizan y producen datos.

La disciplina jurídica de dichos fenómenos, como es el caso del GDPR pero también del AI Act, muchas veces se construye de manera neutral con respecto a las tecnologías a las cuales se aplica, para hacer frente

[37] Vid. por ejemplo: Tribunal de Justicia de la Unión Europea, sent. 4 de julio de 2023, Meta Platforms and Others (General terms of use of a social network), C-252/21, EU:C:2023:537, párr. 106.

[38] Comité europeo de protección de datos personales, Dictamen 28/2024, párr. 70 sigs.

[39] Comité europeo de protección de datos personales, Dictamen 28/2024, párr. 76 sigs.

[40] Como lo define el citado Dictamen 28/2024 (párr. 18):
Web scraping' es una técnica comúnmente utilizada para recopilar información de fuentes en línea de acceso público. La información que se extrae, por ejemplo, de servicios como los medios de comunicación, las redes sociales, los debates en foros y los sitios web personales, puede contener datos personales.

[41] Comité europeo de protección de datos personales, Dictamen 28/2024, párr. 96 sigs.

[42] Por ejemplo la autoridad de supervisión de datos personales de Belgica (vid. Data Protection Authority of Belgium, General Secretariat, Artificial Intelligence Systems and the GDPR A Data Protection Perspective, 2024) entrega este ejemplo:
> Una compañía de seguros de vida, que implementa un sistema de IA para calcular las primas de los seguros de vida, debe garantizar que el sistema cumple con las prohibiciones del GDPR y la Ley de IA en materia de tratamiento de determinados tipos de datos personales. Esto incluye categorías especiales de datos personales, como el origen racial o étnico, las opiniones políticas, las creencias religiosas, la salud, etc. Esto es importante para cumplir con la protección de los datos personales sensibles del GDPR y el énfasis de la Ley de IA en la prevención de resultados discriminatorios.

a la imprevisibilidad de la evolución tecnológica (Mitrou, 2018, p. 26). Sin embargo, en realidad, cada tecnología que trata y produce datos crea problemas específicos que nacen y cambian con mayor rapidez que las consiguientes respuestas éticas, jurídicas y sociales (Fosch et al., 2018, p. 304). Por consiguiente, el uso de la inteligencia artificial plantea continuamente problemas nuevos.[43]

Desde el punto de vista ético-jurídico, el tratamiento de datos por las tecnologías supone muchas cuestiones que solo parcialmente pueden solucionarse con normas específicas como el AI Act, el GDPR y otras normatividades. Esto se observa, por ejemplo, en temas como la reglamentación del mercado, la seguridad, la protección de los consumidores y la propiedad intelectual, que tienen respectivamente enfoques y objetivos distintos (Ruschemeier, 2025).[44]

Comprender los vínculos y contrastes entre estas regulaciones es crucial para garantizar su cumplimiento y fomentar la innovación responsable en el campo de la inteligencia artificial (Busch et al., 2024; Veale & Borgesius, 2021).

En particular, como se ha visto, el uso de la inteligencia artificial representa un desafío para la aplicación de los principios del tratamiento de datos personales y puede hacer necesaria la elaboración de nuevas soluciones de aplicación para salvaguardar la privacidad de la información y otros derechos fundamentales.[45]

Por otro lado, la aplicación conjunta de legislaciones diferentes puede exigir cumplir con muchos requisitos técnicos y estándares normativos lo cual incrementa los costes operativos y conlleva un creciente riesgo de incumplimiento. Eso puede tener un *chilling effect* (un efecto disuasorio) que desincentiva el desarrollo tecnológico[46] y constituiría, en definitiva, un límite al acceso de la ciudadanía europea a las nuevas tecnologías.

Sin embargo, la aplicación conjunta de las diferentes normativas puede basarse en principios y reglas comunes, como el principio de responsabilidad; la necesidad de elaborar documentos para demostrar el cumplimiento; la ética por diseño; una estructura de *governance* pública multinivel; la certificación y, por último, el control de sujetos independientes.[47]

Además, se podrán realizar importantes sinergias entre las fuentes jurídicas. Por ejemplo, la aplicación de los principios del artículo 5 GDPR (como, la minimización) puede impulsar la creación de sistemas de inteligencia artificial más eficientes y sustentables, como destacan los documentos de las autoridades europeas de protección de datos personales. En cambio, el AI Act agrega al tratamiento de datos otros

43 Por ejemplo, considérese el caso de la interación entre personas e IA, vid. Saracini et al., 2025; Burzagli et al., 2025.

44 Por ejemplo, el GDPR enfatiza la protección de datos y los derechos individuales asociados (Artzt, & Viet Dung, 2022), mientras el AI Act es un marco regulatorio de bienes y servicios vinculados a sistemas de IA y que está basado en una clasificación del riesgo en función del potencial para causar daño (Wang & Haak, 2024).

45 Consejo de Europa, Report on Artificial Intelligence -Artificial Intelligence and Data Protection: Challenges and Possible Remedies, September 2018, p. 9.

46 Sobre el punto hay diferentes opiniones: según un estudio del Centre for Data Innovation (How Much Will Artificial Intelligence Act Cost Europe?, 2021, disponible en https://www2.datainnovation.org/2021-aia-costs.pdf) los costes de cumplimiento derivados de la ley sobre la IA provocarían un efecto disuasorio en la inversión en IA en Europa y podrían disuadir especialmente a las pequeñas y medianas empresas (PYMES) de desarrollar sistemas de IA de alto riesgo. Según el estudio, la ley sobre la IA costaría a la economía europea 31 000 millones de euros en los próximos cinco años y reduciría las inversiones en IA en casi un 20 %. Sin embargo, estas estimaciones de los costes de cumplimiento fueron cuestionadas por los expertos del CEPS, Centro de Estudios Políticos Europeos (Clarifying the costs for the EU's AI Act, 2021, https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/?mc_cid=1b1e61c5af&mc_eid=9a740783cd).

47 Vid. el artículo 8.3. de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas; Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, cit. Sobre las caracteristas, los desafíos de la auditoría en los sistemas de IA, vid. Mökander, 2023.

principios no considerados por el GDPR, como la supervisión humana —más allá de lo previsto por el artículo 22 GDPR en materia de decisiones automatizadas—(Sarra, 2024, p. 46) y una atención más precisa y detallada a la calidad de los datos, en lugar de una referencia genérica a la exactitud contenida en el GDPR (Artzt & Viet Dung, 2022). La aplicación convergente de diferentes disciplinas puede apoyar una interpretación no neutral, sino adecuada a la tecnología, de principios específicos.[48]

Como destaca el Consejo de Europa,[49] se debe adoptar una visión más amplia de los posibles resultados del tratamiento de datos, que debería tener en cuenta los derechos humanos y los otros intereses, así como el funcionamiento de las democracias y la promoción de valores sociales y éticos.

De hecho, las diferentes normativas europeas comparten el objetivo común de desarrollar tecnologías "éticas",[50] es decir con un enfoque orientado a los valores en la reglamentación y en el diseño de productos y servicios (Mitrou, 2018, p. 74). Perspectiva que debe ser el resultado de una colaboración entre los operadores y los actores sociales incluyendo en ello a las personas expertas y las instituciones académicas.[51]

Bibliografía citada

Artzt, M., & Viet Dung, T. (2022). Artificial Intelligence and data protection: how to reconcile both areas from the european law perspective. *Vietnamese Journal of Legal Sciences*, *7*(2), 39–58. https://doi.org/10.2478/vjls-2022-0007

Benlloch Domènech, C., & Sarrión Esteve, J. (2022). Los derechos fundamentales ante las aporías de la era digital. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, *(46)*, 3–28. https://doi.org/10.22201/iij.24484881e.2022.46.17046

Burzagli, L., Cornejo-Plaza, M. I., Colcelli, V., & Cippitani, R. (2025). Uso de sistemas de Inteligencia Artificial generativa en la educación: evaluación éticojurídica de una aplicación concreta. *Revista de Educación y Derecho*, *(32)*. https://doi.org/10.1344/REYD2025.32.51543

Busch, F., Kather, J. N., Johner, C., Moser, M., Truhn, D., Adams, L. C., & Bressem, K. K. (2024). Navigating the European Union Artificial Intelligence Act for Healthcare. *Npj Digital Medicine*, *7*(1). https://doi.org/10.1038/s41746-024-01213-6

Buttarelli, G. (2016, 8 de noviembre). *A smart approach: counteract the bias in artificial intelligence*. European Data Protection Supervisor (EDPS). https://www.edps.europa.eu/press-publications/press-news/blog/smart-approach-counteract-bias-artificial-intelligence_en

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law and Security Review*, *34*(2), 257–268. https://doi.org/10.1016/j.clsr.2018.01.004

Bygrave, L. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Cippitani, R. (Ed.). (2012). *El Derecho privado de la Unión Europea desde la perspectiva de la Sociedad del Conocimiento*. ISEG.

Cippitani, R. (2018). Genetic research and exceptions to the protection of personal data. En R. Arnold, R. Cippitani, & V. Colcelli (Eds.), *Genetic information and individual rights* (pp. 54–79). Universität Regensburg. https://doi.org/10.5283/epub.36785

[48] Como se observa a proposito del principio de exactitud, en el contexto de la IA generativa, su aplicación probablemente se centrará en las inexactitudes significativas, en lugar de exigir la corrección absoluta de todos los resultados: v. Novelli et al., 2024, p. 7.

[49] Consejo de Europa, Guidelines on Artificial Intelligence and data protection, 25 de enero 2019.

[50] Comisíon Europea, Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, 25 de noviembre de 2021.

[51] Consejo de Europa, Guidelines on Artificial Intelligence and data protection, ob. cit., apartados III.6, III.7 y III.8.

Cippitani, R. (2023b). La noción de "seguridad" en el Derecho de la Unión Europea. *Criminogenesis*, 163–181.

Cippitani, R., & Castrogiovanni, L. (2023). ChatGpt a la prueba del derecho de la Unión Europea: protección de datos personales y otras cuestiones ético-jurídicas. En M. I. Cornejo Plaza & E. Isler Soto (Eds.), *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Rubicón Editores.

Colcelli, V., Cippitani, R., Brochhausen-Delius, C., & Arnold, R. (Eds.). (2023). *GDPR requirements for biobanking activities across Europe*. Springer. https://doi.org/10.1007/978-3-031-42944-6

Cornejo-Plaza, M. I. (2021). Neuroderecho(s): propuesta normativa de protección al uso inadecuado de neurotecnologías disruptivas. *Revista Jurisprudencia Argentina*, *XXIII* (número especial de Bioética), 49–62.

Cornejo-Plaza, M. I., & Cippitani, R. (2023). Consideraciones éticas y jurídicas de la IA en Educación Superior: Desafíos y Perspectivas. *Revista de Educación y Derecho (Education and Law Review)*, *(28)*. https://doi.org/10.1344/REYD2023.28.43935

Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: Neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, *15*. https://doi.org/10.3389/fpsyg.2024.1330439

Finck, M., & Biega, A. J. (2021). *Reviving purpose limitation and data minimisation in personalisation, profiling and decision-making systems*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3749078

Fosch Villaronga, E., Kieseberg, P., & Tiffany, L. (2018). Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten. *Computer Law and Security Review*, *34*(2), 304–313.

Irion, K. (2016). A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection. En *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (pp. 873–890). Nomos.

Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI & Society*, *34*, 509–533. https://doi.org/10.1007/s00146-017-0758-8

Kamarinou, D., Millard, C., & Singh, J. (2016). *Machine learning with personal data.* Queen Mary School of Law Legal Studies Research Paper No. 247/2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811

Mantelero, A. (2014). The future of consumer data protection in the EU Re-thinking the «notice and consent» paradigm in the new era of predictive analytics. *Computer Law & Security Review*, *30*(6), 643–660.

Martínez, R. (2019). Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo. *Revista Catalana de Dret Públic*, *(58)*, 64–81. https://dialnet.unirioja.es/servlet/articulo?codigo=7005057&orden=0&info=link

Mayta-Tovalino, F., Rospigliosi-Lazo, A. C., Arana-Torres, E., & Tello-Sifuentes, S. (2024). Análisis cienciométrico sobre el uso de ChatGPT, inteligencia artificial o agente conversacional inteligente en la función de formación médica. *Educación Médica*, *25*(2), 100873.

Mitrou, L. (2018). *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* (SSRN Abstract No. 3386914). https://ssrn.com/abstract=3386914

Mökander, J. (2023). Auditing of AI: Legal, Ethical and Technical Approaches. *Digital Society*, *2*(49). https://doi.org/10.1007/s44206-023-00074-y

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, 106066. https://doi.org/10.1016/j.clsr.2024.106066

Reed, C. (2018). How Should We Regulate Artificial Intelligence? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128). https://doi.org/10.1098/rsta.2017.0360

Ruschemeier, H. (2025). Generative AI and data protection. *Cambridge Forum on AI: Law and Governance*, *1*(e6), 1–16. https://doi.org/10.1017/cfl.2024.2

Sacramed, M. T. (2024). Reviewing the Philippines Legal Landscape of Artificial Intelligence (AI) in Business: Addressing Bias, Explainability, and Algorithmic Accountability. *International Journal of Research and Innovation in Social Science*, *8*(5), 2506. https://doi.org/10.47772/ijriss.2024.805181

Saracini, C., Cornejo-Plaza, M. I., & Cippitani, R. (2025). Techno-emotional projection in human–GenAI relationships: a psychological and ethical conceptual perspective. *Frontiers in Psychology*, *16*. https://doi.org/10.3389/fpsyg.2025.1662206

Sarra, C. (2025). Artificial Intelligence in Decision-making: A Test of Consistency between the "EU AI Act" and the "General Data Protection Regulation." *Athens Journal of Law*, *11*(1), 45. https://doi.org/10.30958/ajl.11-1-3

Taylor, M. (2012). *Genetic data and the law: A critical perspective on privacy protection*. Cambridge University Press.

van Daalen, F., Jacquemin, M., van Soest, J., Stahl, N., Townend, D., Dekker, A., & Bermejo, I. (2025). A critique of current approaches to privacy in machine learning. *Ethics and Information Technology*, *27*(32). https://doi.org/10.1007/s10676-025-09843-4

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97. https://doi.org/10.9785/cri-2021-220402

Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law*, *8*(4), 318–337.

Wang, B., & Haak, D. (2024). Regulating Artificial Intelligence in the European Union and the United States. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsrhs.v13i2.6798

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J. W., da Silva Santos, L. B., Bourne, P. E., Bouwman, C. L., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Faulkes, S. C., Gledhill, P., ... Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(160018). https://doi.org/10.1038/sdata.2016.18

Normas citadas

Tratados

Tratado de Funcionamiento de la Unión Europea (s.f.).

Tratado de la Unión Europea (s.f.).

Carta de derechos

Carta de los Derechos Fundamentales de la Unión Europea (s.f.).

Directivas

Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

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

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital.

Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.

Reglamentos

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).

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018.

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 ("Data Governance Act").

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 ("Data Act").

Reglamento (UE) 2024/982 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, relativo a la búsqueda y al intercambio automatizados de datos para la cooperación policial, y por el que se modifican las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los Reglamentos (UE) 2018/1726, (UE) 2019/817 y (UE) 2019/818 del Parlamento Europeo y del Consejo (Reglamento Prüm II).

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.

Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud.

Decisiones

Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE.

Otros documentos citados

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

AESGP, AICI - Associazione Italiana Cistite Interstiziale, Alliance for Regenerative Medicine, BBMRI-ERIC, Biomedical Alliance in Europe, Cancer Patients Europe, COCIR, Deshre, DIGITALEUROPE, EATRIS, ECHAlliance, ECL - Association of European Cancer Leagues, EFN - European Federation of Nurses Associations, EFPIA - European Federation of Pharmaceutical Industries and Associations, EHA - European Hematology Association, EHTEL, ELF - European Lung Foundation, ESCRS - European Society of Cataract & Refractive Surgeons, EU EYE, ... , & WFIPP - World Federation of Incontinence and Pelvic Problems. (2023). *Stakeholder coalition calls for legislative refinement of the EHDS*. https://uroweb.org/news/stakeholder-coalition-calls-for-legislative-refinement-of-the-ehds

Centre for Data Innovation. (2021). *How Much Will Artificial Intelligence Act Cost Europe?* https://www2.datainnovation.org/2021-aia-costs.pdf

CEPS, Centro de Estudios Políticos Europeos (2021). *Clarifying the costs for the EU's AI Act*. https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/?mc_cid=1b1e61c5af&mc_eid=9a740783cd

CNIL (Commission nationale de l'informatique et des libertés) (2017). *Comment permettre à l'homme de garder la main? - Les enjeux éthiques des algorithmes et de l'intelligence artificielle*.

Comisión Europea (1993). *Libro Blanco "Crecimiento, competitividad, empleo"*. (COM(93) 700 final).

Comisión Europea (2010). *Comunicación "EUROPA 2020 Una estrategia para un crecimiento inteligente, sostenible e integrador"*. (COM/2010/2020 final).

Comisión Europea (2016). *Comunicación "Digitalización de la industria europea Aprovechar todas las ventajas de un mercado único digital"*. (COM(2016) 180 final).

Comisión Europea (2020a). *Comunicación "Una estrategia europea para los datos"*. (COM(2020) 66 final).

Comisión Europea (2020b). *Comunicación sobre la configuración del futuro digital de Europa*. (COM(2020) 67 final).

Comisión Europea (2020c). *Libro Blanco sobre la inteligencia artificial*. (COM(2020) 65 final).

Comisión Europea (2021). *Comunicación "Brújula Digital 2030: el enfoque de Europa para el Decenio Digital"*. (COM(2021) 118 final).

Comité europeo de protección de datos personales (2019). *Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados* (Versión 2.0).

Comité europeo de protección de datos personales (2024a). *Report of the work undertaken by the ChatGPT Taskforce*.

Comité europeo de protección de datos personales (2024b). *Dictamen 28/2024 sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA*.

Consejo de Europa (2018). *Report on Artificial Intelligence -Artificial Intelligence and Data Protection: Challenges and Possible Remedies*.

Data Protection Authority of Belgium, General Secretariat (2024). *Artificial Intelligence Systems and the GDPR: A Data Protection Perspective*. https://www.autoriteprotectiondonnees.be/publications/artificial-intelligence-systems-and-the-gdpr---a-data-protection-perspective.pdf

European Data Protection Supervisor (2024). *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*. https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en

European Group on Ethics in Science and New Technologies (2018). *Artificial Intelligence, Robotics and 'Autonomous' Systems*.

Garante italiano per la protezione dei dati personali (2024a). *Provvedimento del 11 de enero 2024* [no. 9977020].

Garante italiano per la protezione dei dati personali (2024b). *Provvedimento del 2 de noviembre de 2024* [no. 10085455].

Grupo de expertos de alto nivel sobre IA en sus Directrices éticas para una inteligencia artificial confiable (2019). *Directrices éticas para una inteligencia artificial confiable*. Comisión Europea. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60656

Parlamento Europeo (2021). *Resolución del 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL))* (DO C 404 de 6.10.2021).

Jurisprudencia citada

Conseil Constitutionnel (2018). *Sentencia n.º 2018-765* (12 de junio de 2018).

Consiglio di Stato (2019). *Sentenza n.º 2270* (4 de abril de 2019).

Consiglio di Stato (2021). *Sentenza n.º 8472* (13 de diciembre de 2021).

Tribunal de Distrito de La Haya (Países Bajos) (2020). *Sentencia* (5 de febrero de 2020).

Tribunal de Justicia de la Unión Europea (2023). *Sentencia Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537 (4 de julio de 2023).