Estudios de Deusto

Revista de Derecho Público

Vol. 74/1 enero-junio 2026

DOI: https://doi.org/10.18543/ed7412026

ESTUDIOS

LA PROTECCIÓN DE LOS DATOS PERSONALES EN LOS TIEMPOS DE LA IA: ¿CABE PROMOVER UN ENFOQUE ESENCIALMENTE NORMATIVO EN TIEMPOS DE RENUNCIA A LA PRIVACIDAD?

Personal Data Protection in the Age of AI: Can an Essentially Normative Approach Be Defended in an Era of Privacy Renunciation?

Federico de Montalvo Jääskeläinen
Profesor propio ordinario de Derecho Constitucional
ICADE - Universidad Pontificia de Comillas, Madrid. España
https://orcid.org/0000-0002-9272-7359

https://doi.org/10.18543/ed.3578

Fecha de recepción: 24.05.2025
Fecha de aceptación: 18.12.2025
Fecha de publicación en línea: junio 2026

LA PROTECCIÓN DE LOS DATOS PERSONALES EN LOS TIEMPOS DE LA IA: ¿CABE PROMOVER UN ENFOQUE ESENCIALMENTE NORMATIVO EN TIEMPOS DE RENUNCIA A LA PRIVACIDAD?

Personal Data Protection in the Age of AI: Can an Essentially Normative Approach Be Defended in an Era of Privacy Renunciation?

Federico de Montalvo Jääskeläinen[1]
Profesor propio ordinario de Derecho Constitucional
ICADE - Universidad Pontificia de Comillas, Madrid. España
https://orcid.org/0000-0002-9272-7359

https://doi.org/10.18543/ed.3578

Fecha de recepción: 24.05.2025
Fecha de aceptación: 18.12.2025
Fecha de publicación en línea: junio 2026

El trabajo algorítmico de cálculo no es narrativo, sino puramente aditivo. Los algoritmos numeran, pero no narran. El paso del mito al dataismo es el paso de la narración a la mera enumeración

Byung-Chul Han

Resumen

La relación entre la IA y el uso secundario de datos es inescindible, de manera que puede afirmarse que los datos son la *energía* que permite que el *motor* de la IA pueda desarrollarse y funcionar. La IA es esencialmente una tecnología de procesamiento avanzado de la información y su proceso completo exige de una primera fase

[1] Email: fmontalvo@comillas.edu

de recolección de datos, previa a las siguientes de construcción e implementación del modelo. Por ello, las cuestiones relativas al derecho a la privacidad y a la confidencialidad de los datos cobran de nuevo una especial relevancia en este contexto. Para su debida protección se ha propuesto un tradicional enfoque normativo que regule tales derechos ante los riesgos y nuevos conflictos que supone la IA. Sin embargo, este enfoque olvida que tales derechos han sido, en gran parte, objeto de renuncia por una gran parte de la población que ha primado la utilidad de las aplicaciones derivadas de las nuevas tecnologías frente a sus derechos a la privacidad y confidencialidad de datos. Por ello, es conveniente un enfoque formativo basado en la denominada alfabetización digital.

Palabras clave

Inteligencia artificial, protección de datos, privacidad, uso secundario, seudonimización, alfabetización digital

Abstract

The relationship between AI and the secondary use of data is inextricable, such that data may be described as the fuel that powers the AI engine. AI is, in essence, an advanced information-processing technology, and its full development necessarily involves an initial phase of data collection, preceding the subsequent stages of model construction and implementation. Accordingly, issues concerning the right to privacy and data confidentiality acquire renewed significance in this context. In response, a traditional regulatory approach has been proposed to safeguard such rights against the risks and emerging conflicts posed by AI. However, this approach overlooks the fact that these rights have, to a large extent, been voluntarily relinquished by a significant portion of the population, which has prioritized the utility of new technological applications over the protection of privacy and data confidentiality. Therefore, a complementary educational approach, grounded in so-called digital literacy, is advisable.

Keywords

Artificial Intelligence, Data Protection, Privacy, Secondary Use, Pseudonymisation, Digital Literacy

Sumario: I. Big Data e IA: una relación inescindible y circular. II. El derecho a la protección de datos personales. III. Garantías legales de protección de la privacidad y la confidencialidad de los datos. IV. La posible falta de virtualidad del marco de garantías asentado, sustancialmente, en el consentimiento informado en el contexto de la IA. V. Otras propuestas para la protección de los datos en el contexto de la IA. VI. La alfabetización digital como gran reto. VII. Bibliografía.

I. BIG DATA E IA: UNA RELACIÓN INESCINDIBLE Y CIRCULAR

La relación entre la IA y el Big Data[2] o uso masivo de datos es inescindible, de manera que puede afirmarse que los datos son la *energía* que permite que el *motor* de la IA pueda desarrollarse y funcionar. Un sistema de IA como "sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue"[3], necesita información de entrada, es decir, datos para generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales. La IA es esencialmente una tecnología de procesamiento avanzado de la información y su proceso completo exige de una primera fase de recolección de datos, previa a las siguientes de construcción e implementación del modelo. La IA vive de los datos insertos previos (Al Hasani Maturano, 2024, p. 30).

En palabras de la Comisión de la UE, para poder desarrollar la IA se precisan enormes cantidades de datos. El aprendizaje automático, que es un tipo de IA, consiste en la identificación de patrones en los datos disponibles y en la aplicación subsiguiente del conocimiento adquirido a nuevos datos. Y cuanto mayor es el conjunto de datos, más fácil resulta descubrir las relaciones entre ellos, incluso las más sutiles. En lo que atañe a la utilización de la IA, los entornos ricos en datos también brindan más oportunidades. Ello se debe a que los datos son los que permiten al algoritmo aprender acerca de su entorno e interactuar con él. Así pues, el acceso a los datos es un factor clave para una IA competitiva[4].

[2] El término Big Data viene referido a los macrodatos y se caracteriza por las denominadas cuatro V, volumen, variedad, velocidad y valor.

[3] Vid. art. 3 del Reglamento UE de la IA.

[4] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Inteligencia artificial para Europa*, 24 de abril de 2018, pp. 11 y 12.

La IA se relaciona, por tanto, de forma clara con el Big Data. Lo necesita para desarrollar sus funcionalidades, ya que se nutre de la gran cantidad de datos recopilados para entrenar modelos de aprendizaje automático y tomar decisiones basadas en patrones y correlaciones. Esta sinergia permite a la IA realizar tareas como el procesamiento de lenguaje natural, la visión por computadora y la toma de decisiones predictivas con un alto grado de precisión (Cotino Hueso, 2017; y Pérez-Ugena, 2024, p. 311). Analizando grandes conjuntos de datos con el objetivo de identificar patrones, la IA trata de imitar ciertos procesos cognitivos típicos de la capacidad humana de resolución de problemas[5].

Preguntarse por la regulación jurídica de la IA exige, pues, ampliar el foco, incluyendo también las cuestiones y riesgos derivados del Big Data, en especial, lo que se refiere a la privacidad y la confidencialidad de los datos. Como dijera Lorenzo Cotino, en las etapas inmediatamente previas a la aprobación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 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) –en adelante, Reglamento UE de la IA–, "hoy por hoy el régimen de protección de datos es la principal respuesta regulatoria frente a los sistemas de IA" (Cotino Hueso, 2023, p. 6).

Los grandes datos son generados por humanos, también biométricamente, producidos máquina a máquina, producto de grandes transacciones o del uso de la web y redes sociales. Billones de mensajes de WhatsApp, correos electrónicos, contenidos en Facebook, Twitter (X), búsquedas en Google, vídeos en YouTube. Los datos masivos se generan por la navegación en internet, las comunicaciones del internet de las cosas, comunicaciones entre máquinas, industrias, estaciones meteorológicas, etc. por lo general vinculadas a medidores y sensores de temperatura, luz, altura, presión, sonido, localización, GPS, así como en el entorno de tecnologías RFID, wifi o bluetooth. A sumar a los datos biométricos, normalmente vinculados al ámbito de seguridad, pero también de sanidad (escáneres de retina, de huellas digitales, o lectores de cadenas de ADN, monitoreos médicos de todo tipo, etc.) (Cotino Hueso, 2017, p. 133). Y ahora también los denominados neurodatos derivados de las nuevas neurotecnologías[6].

[5] Dicasterio para la Doctrina de la Fe y del Dicasterio para la Cultura y la Educación, Nota sobre la relación entre la inteligencia artificial y la inteligencia humana, Ciudad del Vaticano, 28.01.2025. Puede accederse al documento a través del siguiente enlace: https://press.vatican.va/content/salastampa/es/bollettino/pubblico/2025/01/28/280125a.html.

[6] Las Directrices de la Comisión sobre las prácticas de inteligencia artificial prohibidas que se establecen en el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia

La considerable cantidad de datos recopilados y analizados por los usuarios, la ubicuidad y continuidad del proceso de comunicación en el llamado ecosistema móvil (incluidos proveedores, fabricantes, vendedores y usuarios) y la interconectividad y accesibilidad simultánea por una variedad de motores de análisis sin apenas fricción, ofrecen una estructura que facilita el análisis conjunto de todos esos datos y, por tanto, el avance del desarrollo de algoritmos y de la IA. Esta explotación masiva puede llevarse a cabo, además, interconectando e interrelacionando no solo los datos de fuentes oficiales o estructurados, en sentido estricto, sino también los que no son considerados como tales, los no tradicionales o no estructurados, en especial, los que se producen en las redes de consumo ordinario.

Así, destacan ahora los datos que generan nuevas tecnologías como *apps* y *wearables*, es decir, dispositivos electrónicos y aparatos "vestibles", que se incorporan sobre alguna parte de nuestro cuerpo (ropa, gafas, pulseras, relojes, …) para producir datos sobre actividades, conductas o hábitos de vida, producen, cada segundo, millones de datos[7]. Los wearables están dotados de sensores que permiten recoger y emitir datos de forma constante y se pueden clasificar en tres categorías principales: sensores de movimiento (convierten el movimiento mecánico en una señal eléctrica), fisiológicos (utilizan componentes ópticos, eléctricos, acústicos o de detección térmica para medir parámetros vitales como la frecuencia cardíaca, la temperatura, la presión arterial o la saturación de oxígeno en sangre, la actividad bioeléctrica como electrocardiografía o electroencefalografía) y bioquímicos (se utilizan para medir sustancias químicas como la glucosa, electrólitos) (Alós y Puig-Ribera, 2021)[8]. Estas fuentes de información alternativas, provenientes de aplicaciones móviles y generadas por diferentes dispositivos portátiles,

Artificial) recuerda que hay juegos que pueden utilizar neurotecnologías que posibilita la IA e interfaces cerebro-máquina que permiten a los usuarios controlar un juego o partes del mismo con un casco que detecte la actividad cerebral. Y así la IA puede utilizarse para entrenar el cerebro del usuario de forma subrepticia y sin su conocimiento para revelar o extraer de los datos neuronales información que puede ser muy intrusiva o sensible (por ejemplo, información bancaria personal, información íntima, etc.) de un modo que pueda provocarles perjuicios considerables (pág. 25).

[7] Se calcula que existen más de 3,48 millones de aplicaciones móviles disponibles en la plataforma Google Play y 2,22 millones en el Apple App Store, de las que más de un millón están relacionadas con la salud, el estado fisico, la alimentación y el bienestar general.

[8] El Comité Nacional de Bioética de Italia, en su Informe sobre los aspectos bioéticos de las aplicaciones móviles de salud de 28 de mayo de 2015, destaca el papel que ya están ocupando las aplicaciones móviles o *apps* como fuente de generación de datos. Puede accederse a dicho Informe a través de la página web del Comité Nacional de Bioética de Italia, en http://bioetica.governo.it/it/.

además de los mensajes de las redes sociales generales o los metadatos (datos relacionados con la generación de otros datos, como es el caso de la geolocalización de los datos que genera un dispositivo), cada vez cobran más importancia (Alcalde Bezhold y Alfonso Farnós, 2019, p. 61). El Big Data permite a los investigadores integrar y agregar información diversa de múltiples fuentes[9].

Se habla ya de un escenario de altísimo nivel de contaminación digital, debido al volumen de datos que se recolectan y la creciente capacidad de interrelación y analítica en masa, que se encuentra en un punto de no retorno (Castillo Parrilla, 2023, p. 58). Datos hay muchos, quizás, demasiados ya, por lo que la cuestión se centra ahora en su calidad para permitir desarrollar una IA fiable.

La digitalización de la realidad y el protagonismo del dato personal que ello produce han sido, pues, el presupuesto necesario para que la IA haya podido desarrollarse. Sin datos no habría algoritmos y sin éstos no habría IA.

Esta directa relación entre datos e IA se recoge en el propio Reglamento UE de IA cuando manifiesta que "no debe entenderse que el presente Reglamento constituye un fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, en su caso, salvo que el presente Reglamento disponga específicamente otra cosa" (Considerando 63), añadiendo que "los datos de alta calidad y el acceso a datos de alta calidad desempeñan un papel esencial a la hora de proporcionar una estructura y garantizar el funcionamiento de muchos sistemas de IA, en especial cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione del modo previsto y en condiciones de seguridad y no se convierta en una fuente de algún tipo de discriminación prohibida por el Derecho de la Unión. Es preciso 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).

El propio Reglamento incluye entre sus definiciones contenidas en el artículo 3, diferentes clases de datos vinculados a la IA:

– "datos de entrenamiento": los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;
– "datos de validación": los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o el sobreajuste;

[9] German Ethics Council, *Big Data and health. Data sovereignty as the shaping informational freedom*, *cit.*, p. 10.

– "conjunto de datos de validación": un conjunto de datos independiente o una parte del conjunto de datos de entrenamiento, obtenida mediante una división fija o variable;
– "datos de prueba": los datos usados para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio;
– "datos de entrada": los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida;
– "datos biométricos": los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos;
– "datos operativos sensibles": los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales.

Así pues, el Reglamento UE de la IA no puede considerarse como una norma aislada, sino como una norma que integra un corpus jurídico del que forman parte, principalmente, ésta y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) –en adelante, Reglamento UE de protección de datos–, como normas generales, al margen de otras normas más sectoriales, destacando también el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, aunque esta norma, desde la perspectiva del debate que nos ocupa, es menos relevante, ya que la materia objeto de regulación, los datos no personales, no deben plantear cuestiones relativas a la privacidad.

Y como señala el Reglamento UE de protección de datos (considerandos 6 y 7), la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar

aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

Por ello, siguiendo con el Reglamento, estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

El Grupo Independiente de Expertos de Alto Nivel sobre IA en sus Directrices éticas para una IA fiable de 2019 señala a este respecto que "la privacidad es un derecho fundamental que se ve especialmente afectado por los sistemas de IA, y que guarda una estrecha relación con el principio de prevención del daño. La prevención del daño a la privacidad también requiere una adecuada gestión de los datos, que abarque la calidad y la integridad de los datos utilizados, su pertinencia en contraste con el ámbito en el que se desplegarán los sistemas de IA, sus protocolos de acceso y la capacidad para procesar datos sin vulnerar la privacidad"[10].

Los riesgos para los derechos fundamentales derivados del tratamiento de datos son también destacados por el Reglamento UE de la IA: "El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados, sin perjuicio de los requisitos en materia de gobernanza de datos establecidos en el presente Reglamento" (Considerando 69).

El Dictamen 28/2024 del Comité Europeo de Protección de Datos sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA[11] recuerda, además, que si bien "los modelos de IA entrenados con datos personales sue-

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

[11] Puede accederse al mismo a través del siguiente enlace: https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_es_0.pdf.

len estar diseñados para hacer inferencias sobre personas distintas de aquellas cuyos datos personales se utilizaron para entrenar el modelo de IA", algunos de ellos sí "están diseñados específicamente para proporcionar datos personales relativos a las personas cuyos datos personales se utilizaron para entrenar el modelo, o de alguna manera para que dichos datos estén disponibles. En estos casos, dichos modelos de IA incluirán intrínsecamente (y normalmente necesariamente) información relativa a una persona física identificada o identificable, por lo que implicarán el tratamiento de datos personales" (apartado 29). Incluso, los modelos de IA pueden ser capaces de "conservar la información original de esos datos, que en última instancia puede ser extraída u obtenida de otro modo, directa o indirectamente, del modelo. Siempre que la información relativa a personas identificadas o identificables cuyos datos personales se utilizaron para entrenar el modelo pueda obtenerse de un modelo de IA con medios que sea razonablemente probable que se utilicen, puede concluirse que dicho modelo no es anónimo" (apartado 30). Así pues, los modelos de IA suponen un reto cualificado para la protección de datos personales en la medida que las posibilidades de levantar el anonimato son reales.

Pero no sólo los datos y su uso masivo nutren a la IA, sino que ésta también lo hace respecto de aquéllos. Y es que los avances en la elaboración y el análisis de datos que posibilita la IA permiten detectar patrones en el comportamiento y el pensamiento de una persona incluso a partir de una cantidad mínima de informaciones, lo que hace aún más necesaria la privacidad de los datos como salvaguardia de la dignidad y la naturaleza relacional de la persona humana[12].

El uso masivo incrementa el poder tecnológico de la IA y ésta a su vez lo hace respecto de dicho uso masivo. La relación es pues inescindible y circular. Y a este respecto, puede recordarse, también, que la actividad de tratamiento de datos no solo se produce al inicio del proceso de creación de la IA, sino también cuando los algoritmos se aplican a una persona concreta.

Como recuerda Castillo Parrilla, si bien los "perfiles abstractos no son datos personales mientras no están asociados a una persona concreta y, por lo tanto, no les resulta de aplicación las garantías legales del derecho a la protección de datos. Sin embargo, cuando estos perfiles se aplican a una persona concreta ya sí se está realizando un tratamiento de datos personales en la medida en que el perfil abstracto deja de ser tal para convertirse en el perfil en que se ha categorizado a una persona concreta. Esto ya sí es un tratamiento

[12] Dicasterio para la Doctrina de la Fe y del Dicasterio para la Cultura y la Educación, *Nota sobre la relación entre la inteligencia artificial y la inteligencia humana*, Ciudad del Vaticano, 28.01.2025. Puede accederse al documento a través del siguiente enlace: https://press.vatican.va/content/salastampa/es/bollettino/pubblico/2025/01/28/280125a.html.

de datos" (Castillo Parrilla, 2023, p. 80). Y ello, pese a que la versión en lengua española del Reglamento UE de protección de datos hable en su artículo 4.4 de "elaboración de perfiles", mientras que en la versión de lengua inglesa el término sea "profiling", perfilado. Y es que, como señala también Castillo Parrilla, "la aplicación de un perfil abstracto a una persona concreta es una actividad de tratamiento de datos como cualquier otra. Se trata de una operación realizada sobre datos personales, ya sea por procedimientos automatizados o no, orientada a evaluar determinadas características de una persona física". Para dicho autor, "da igual aquí si entendemos que la actividad de tratamiento se produce del perfil a la persona o de la persona al perfil", porque "se está estableciendo una relación de semejanza suficientemente relevante entre el perfil abstracto y la persona" (Castillo Parrilla, 2023, p. 80).

Así pues, en este trabajo nos vamos a aproximar a las cuestiones éticas y legales que plantea la IA desde la perspectiva del uso masivo de datos, con los riesgos que ello conlleva para la privacidad de los individuos y la confidencialidad de sus datos. Ello nos permitirá comprobar cómo la principal iniciativa que se está llevando a cabo para proteger tales derechos fundamentales es de naturaleza esencialmente normativa, estableciendo diferentes bases de legitimación y garantías. Sin embargo, muchos de nuestros ciudadanos han renunciado ya a su derecho a la intimidad, primando la utilidad de la aplicación sobre el riesgo de exposición, lo que, como explicaremos al final del trabajo, exigiría complementar el enfoque normativo con un enfoque formativo que permita recuperar una nueva cultura de la intimidad y privacidad. Dicho enfoque formativo sí aparece ya en algunas de las últimas normas sobre la IA, aunque sería preciso acentuar dicho enfoque que, probablemente, sea más eficaz para afrontar los nuevos riesgos que la mera aprobación de normas legales de protección. Una recuperación de la cultura de los derechos.

II. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Como manifestara hace ya varias décadas el Tribunal Constitucional, los riesgos derivados del exceso, de los errores, o del uso incontrolado de información de carácter personal no pueden ser afrontados eficazmente por los particulares afectados a causa de una información insuficiente, pues los ciudadanos se encuentran inermes por la imposibilidad de averiguar qué información sobre sus personas se almacenan. Y, menos aún, pueden conocer y prevenir o perseguir el uso desviado o la diseminación indebida de tales datos, incluso aunque le causen lesiones en sus derechos o intereses legítimos. De aquí que el Convenio europeo de 1981 no se limite a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11; sino que los complete con unas

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 159-200
https://doi.org/10.18543/ed.3578 • http://www.revista-estudios.deusto.es/

garantías para las personas concernidas, que formula detalladamente su art. 8 (STC 254/1993, FJ 4.º).

Y añade en una posterior resolución que, en previsión de los nuevos riesgos que ello pueda originar para la plena efectividad de los derechos de los ciudadanos, se dispone en el art. 18.4 C.E. que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (STC 202/1999, FJ 2.º).

Nos encontramos en el ámbito del Big Data con un derecho *ex novo*, surgido al albur del avance de la tecnología, y que tiene naturaleza propia respecto del derecho a la intimidad. Como ha señalado el Tribunal Constitucional, este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran (STC 292/2000, FJ 5.º).

Y es que el derecho fundamental a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de resguardar su vida privada de una publicidad no querida (STC 292/2000, FJ 5.º). Con el primero se habilita para oponerse a que los datos personales sean tratados. Pero como recuerda Antonio Troncoso, "el tratamiento de datos personales no supone de por sí una injerencia en el derecho fundamental a la protección de datos personales pues es el presupuesto del ejercicio del derecho". Tal injerencia "en el derecho fundamental a la protección de datos personales se produce cuando el tratamiento de datos personales no cumple unas condiciones, es decir, no respeta los principios, los derechos y las obligaciones del responsable" (Troncoso Reigada, 2024, p. 500).

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado (STC 292/2000, FJ 5.º).

Y es interesante recordar que este derecho no es creado por el constituyente, ya que no se proclama expresamente por el tenor del artículo 18.4 que se limita a advertir de los riesgos que la informática conlleva para los derechos y libertades, por lo que "la ley limitará su uso". El derecho se proclama o, en términos más correctos, es deducido por el Tribunal Constitucional de dicho precepto.

En todo caso, como recuerda Antonio Troncoso, el derecho a la protección de datos personales, sin negar su carácter autónomo, en la mayoría de los casos que se aplica "se observa su carácter instrumental en relación con la garantía de otros derechos fundamentales". Para el mismo autor, "esto no es consecuencia únicamente de que el derecho a la protección de datos personales, como todos los derechos fundamentales, tenga su fundamento en la dignidad de la persona y el libre desarrollo de la personalidad", sino del hecho de que "el derecho a la protección de datos personales tenga dentro de su naturaleza jurídica su carácter instrumental". La protección de datos personales constituye, pues, "un derecho autónomo, con una sustantividad propia, que en alguna medida también reside en que actúa como garantía institucional de otros derechos" (Troncoso Reigada, 2024, p. 487).

Por otro lado, es importante recordar que el objeto que tutela el derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la

vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo (STC 292/2000, FJ 6.º).

Así pues, el derecho fundamental a la protección de datos personales protege todos los datos personales, sean o no íntimos, incluso aunque sean ya de conocimiento público, ya que, como señala el Tribunal Constitucional Federal alemán, datos insignificantes en sí mismos pueden ofrecer perfiles de personalidad completos mediante sistemas modernos de procesamiento de datos sin grandes gastos de tiempo, dando lugar a lo que se ha dado en llamar «persona de cristal» –*gläserner Mensch*–[13].

Además, el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 292/2000, FJ 6.º).

Por tanto, el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos

[13] Vid. Sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983 sobre el censo (BVerfGE 65, 1; 1 BvR 209/83 y otros).

personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos (STC 292/2000, FJ 7.º).

El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin (STC 292/2000, FJ 5.º).

Y añade el Tribunal Constitucional que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta (STC 202/1999, FJ 2.º).

Y, por consiguiente, la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC 202/1999, FJ 2.º y 292/2000, FJ 5.º).

Como se deriva de las últimas palabras recogidas en esta Sentencia, las garantías no pueden limitarse a lo que se denomina, comúnmente, uso primario, es decir, cuando la información se obtenga directamente del sujeto participante y el uso de los datos es para los fines para los que se pidió autorización de tratamiento, sino, especialmente, para aquellos otros usos distintos, los denominados usos secundarios, cuando la información provenga de datos ya existentes y recabados para un fin distinto, la reutilización de los datos.

III. GARANTÍAS LEGALES DE PROTECCIÓN DE LA PRIVACIDAD Y LA CONFIDENCIALIDAD DE LOS DATOS

¿Cuáles son dichas garantías que exige la debida protección de estos derechos en el ámbito del uso de datos personales?

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 159-200
https://doi.org/10.18543/ed.3578 • http://www.revista-estudios.deusto.es/

Como puede deducirse de lo expresado por el Tribunal Constitucional acerca de las características y facultades que conlleva el derecho a la protección de los datos personales, la principal garantía sería la del consentimiento informado. El acceso y tratamiento de los datos de un individuo exige, ineludiblemente, que medie la previa autorización expresa del individuo. Ello se expresa en el lenguaje de la protección de datos personales como una base de legitimación, pero, desde la teoría general de los derechos fundamentales y del propio Derecho constitucional (a la postre se trata de derechos fundamentales y de sus límites, lo que permite articularlo en un lenguaje propio de dicha categoría) se trataría de garantías.

E insistimos en esta idea de garantía, porque el consentimiento informado no es un derecho en sí, sino una garantía de otro derecho o derechos que, en el caso de los datos personales se refiere, serían la intimidad, privacidad y la protección de datos considerada como derecho[14].

Así, la Carta de Derechos Fundamentales de los ciudadanos de la Unión Europea consagra en su art. 8 el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, exigiendo que los datos personales se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.

El Reglamento UE de protección de datos establece que el consentimiento del titular de los datos a su tratamiento debe ser libre, específico, informado e inequívoco, mediante una declaración o una clara acción afirmativa (artículo 4).

El Considerando 32 del Reglamento menciona que el otorgamiento del consentimiento puede incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad

[14] Recuérdese que el propio Tribunal Constitucional en su Sentencia 37/2011 nos recordaba que, en el ámbito del tratamiento médico, el consentimiento informado operaba como una garantía del derecho a la integridad proclamado en el artículo 15 CE, lo que es plenamente trasladable al ámbito de la protección de datos personales, siendo, en esencia, la misma garantía aunque de un derecho diferente del abordado en dicho caso por el Alto Tribunal: "las garantías que, desde la perspectiva del art. 15 CE, se imponen a toda intervención médica que afecte a la integridad corporal del paciente" (FJ 3.º) o "La información previa, que ha dado lugar a lo que se ha venido en llamar consentimiento informado, puede ser considerada, pues, como un procedimiento o mecanismo de garantía para la efectividad del principio de autonomía de la voluntad del paciente y, por tanto, de los preceptos constitucionales que reconocen derechos fundamentales que pueden resultar concernidos por las actuaciones médicas, y, señaladamente, una consecuencia implícita y obligada de la garantía del derecho a la integridad física y moral, alcanzando así una relevancia constitucional que determina que su omisión o defectuosa realización puedan suponer una lesión del propio derecho fundamental" (FJ 4.º).

de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento", recayendo su prueba en el responsable del tratamiento ("el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales"), según el artículo 7.1.

Eva Gil concluye en su valoración de la regulación del consentimiento contenida en el Reglamento UE de protección de datos que esta norma ha reforzado la figura del consentimiento, "mediante el endurecimiento de los requisitos ya existentes, siendo un claro ejemplo de ello la ampliación de la información que el responsable debe aportar y que está directamente relacionada con el consentimiento informado, que incluye la obligación de comunicar al interesado su derecho a retirar el consentimiento". Y añade, también, "mediante la incorporación de cambios con el ánimo de que supongan garantías adicionales. Entre ellas, la necesidad de que el consentimiento deba prestarse de manera expresa o que el responsable deba ser capaz de demostrar que lo obtuvo" (Gil González, 2020, p. 141).

Cierto es que la garantía del consentimiento informado no es el único instrumento que legitima el tratamiento de datos personales, ya que el artículo 6 del Reglamento UE de protección de datos, relativo a la licitud del tratamiento, recoge junto a éste, otros supuestos legitimadores:

– Cuando el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
– Cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
– Cuando sea necesario para proteger intereses vitales del interesado o de otra persona física;
– Cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
– O cuando sea 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, en particular cuando el interesado sea un niño.

Sin embargo, tras la lectura de estas otras causas de licitud del tratamiento puede comprobarse que realmente existe una única garantía, la del consentimiento informado del titular de los datos, el cual puede operar expresa o tácitamente –mediante una clara acción afirmativa–, y unas excepciones a dicha

garantía que operarían cuando hubiera un conflicto entre el derecho del individuo y el derecho de un tercero o el interés colectivo.

Es decir, las bases de legitimación para el tratamiento de datos personales son varias, pero la garantía del derecho a la protección de datos es única, el consentimiento informado, siendo el resto de bases meras fórmulas de consentimiento tácito o excepciones basadas en conflictos con los derechos de terceros o el interés colectivo. La Ley no puede prever el tratamiento al margen del consentimiento informado, sin que concurra un derecho de un tercero o un interés colectivo que deba prevalecer, superando en estos últimos casos el criterio de la ponderación o el principio de proporcionalidad.

Eso es lo que se deduce de la opinión, por ejemplo, del Abogado General del Tribunal de Justicia de la Unión Europea en el caso Rigas[15], cuando señala que hay tres tipos de bases para el tratamiento de datos: en primer lugar, el consentimiento del interesado. En segundo lugar, las bases descritas en los apartados b)-e), en las que los intereses del responsable del tratamiento se presumen. Por último, la base del apartado f) en la que los intereses legítimos del responsable no se presumen, sino que su existencia debe probarse, y además deben ganar un juicio de ponderación contra los intereses y libertades de los interesados.

La posibilidad de permitir el acceso y tratamiento de datos sobre la base de un fundamento legítimo distinto del consentimiento y previsto por norma con rango de ley debe entenderse, no tanto como una excepción al consentimiento como garantía de la protección de los datos personales, sino como expresión por parte del legislador de la concurrencia de un conflicto entre el derecho a la protección de datos personales y otro derecho fundamental o entre aquél y el interés colectivo. La legitimación por previsión normativa con rango de ley no habilita al legislador a establecer excepciones a la garantía del consentimiento, sino que es expresión de que el derecho a la protección de datos personales, como cualquier otro derecho fundamental, tiene sus límites, pudiendo ceder o verse limitado por obra de la ponderación o de la proporcionalidad. Así, por ejemplo, lo establece nuestro Tribunal Constitucional en la Sentencia 76/2019, en la que se enjuiciaba la inconstitucionalidad de la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, por posibilitar la recopilación por los partidos políticos de datos personales relativos a las opiniones políticas de los ciudadanos.

Es bueno recordar que el derecho a la protección de datos, como el resto de derechos y libertades, incluidos la intimidad y privacidad, no es ilimitado. En palabras nuevamente del Tribunal Constitucional, esos límites o bien pueden ser restricciones directas del derecho fundamental mismo o bien pueden

[15] Vid. Tribunal de Justicia de la Unión Europea (2017): Asunto C-13/16, Rïgas, Opinión del Abogado General, de 26 de enero. ECLI:EU:C:2017:43, párrafos 56-57.

ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (STC 292/2000, FJ 11º).

Y también es importante destacar relevancia que en este campo tiene el concepto legal de expectativa razonable que recoge expresamente el Reglamento UE de protección de datos personales (Considerando 47). A través del mismo se hace referencia a la posibilidad que tendría el interesado de prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que puede producirse una reutilización de sus datos o que ésta no es algo razonablemente descartable.

Este concepto de expectativa razonable cobra, aún, mayor relevancia en el ámbito de los datos personales y la IA. Así, el ya citado Dictamen 28/2024 del Comité Europeo de Protección de Datos sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA[16], recuerda que "las expectativas razonables desempeñan un papel clave en la prueba de ponderación, entre otras cosas debido a la complejidad de la tecnología utilizada en los modelos de IA y al hecho de que puede resultar difícil para los interesados comprender la variedad de usos potenciales de un modelo de IA y el tratamiento de datos que implica". Y, por ello, "la información facilitada a los interesados podrá tenerse en cuenta para evaluar si estos pueden esperar razonablemente que se traten sus datos personales" (apartado 92).

Por otro lado, el ordenamiento jurídico establece un supuesto en el que no operaría el derecho a la protección de datos y, por ende, su garantía a través del consentimiento informado: los datos anonimizados. No es, en sentido estricto, una excepción al consentimiento, sino un contexto *extra legem*, al no tratarse ya de datos personales, de una persona física identificada o identificable. En palabras del Reglamento UE de protección de datos, "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo" (Considerando 26).

Sin embargo, en la práctica la anonimización más que un supuesto concreto se convierte, habitualmente, en un supuesto creado como alternativa para no verse compelido a cumplir con la garantía del derecho a la protección de datos. El responsable cuenta, por tanto, con dos alternativas, bien tratar

[16] Puede accederse al mismo a través del siguiente enlace: https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_es_0.pdf.

datos personales, de persona identificada o identificable, o bien anonimizar los datos y evitar así la operatividad de lo previsto en la regulación. Pero, eso sí, el Reglamento UE de protección de datos aclara que para determinar si una persona física es o no identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Y esta "probabilidad razonable" de reidentificación constituye, como es obvio, un concepto jurídico indeterminado.

Se trata de un sistema de doble opción, en virtud del cual, pueda optarse por el consentimiento o por la anonimización, o lo que viene a ser lo mismo, entre moverse dentro de la normativa de protección de datos personales o quedar fuera de ella.

En todo caso, a estas dos opciones se ha añadido a partir del precitado Reglamento UE sobre protección de datos, una tercera alternativa, la seudonimización que no operaría como excepción o supuesto extra *legem*, como ocurre con la anonimización, sino como garantía alternativa a la del consentimiento informado, aunque, eso sí, acompañada de otros elementos que puedan informar a favor de su utilización en determinados supuestos.

Esta alternativa que incorpora el Reglamento UE de protección de datos es definida por su artículo 4 como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Puede considerarse que esta definición de seudonimización resulta algo paradójica, en la medida que es restrictiva pero amplia al mismo tiempo. Es restrictiva en el sentido de que excluye procesos que no pueden garantizar que los datos personales no se atribuyan a una persona física identificable. Sin embargo, es también amplia como decimos ya que la mera separación de la información adicional del dato parece sujetar el tratamiento de éstos a un régimen jurídico muy próximo o casi similar al del dato anonimizado, lo que se traduce en la no exigencia del consentimiento informado.

En todo caso, la seudonimización cobra un singular protagonismo en el Reglamento UE de protección de datos, y ello, creemos, por dos motivos: para promover de una manera ponderada, pero más flexible la innovación que supone el uso secundario de datos y, en segundo lugar, porque existen

dudas acerca de la verdadera operatividad del consentimiento informado como principal garantía de la privacidad del individuo y de la confidencialidad de sus datos. El propio Reglamento habla, literalmente, de "incentivar la aplicación de la seudonimización en el tratamiento de datos personales" (Considerando 29) y señala, también, que "la aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos" (Considerando 28).

Y debemos recordar que seudonimizar no supone una suerte de *seudoanonimización*, por lo que no puede incluirse, a los efectos de la alternativa entre consentimiento y anonimización, en esta última categoría, sino como una fórmula técnico-legal de recodificación o codificación compleja del dato, sustituyendo unos códigos identificables por otros que no lo sean. Seudonimizar no es anonimización, no es una versión desvirtuada de la anonimización, como ocurre normalmente cuando precedemos la correspondiente palabra con "seudo", sino poner un seudónimo, un código (Romana García y Hernández Pardo, 2018, p. 93). Seudonimizar no puede, por tanto, equipararse a seudoanonimización, como una especie de anonimización algo más débil, sino como la exigencia legal de ocultar el nombre del dato con un seudónimo, es decir, un código, de manera que el concepto equivaldría más al de una disociación más compleja o fuerte[17].

Así, la seudonimización permitiría un uso de los datos, más allá del uso primario, sin un nuevo consentimiento, ya sea expreso o tácito, y sin necesidad de optar por la anonimización. Es, en cierto modo, el modelo que sugiriera hace tres lustros Ohm cuando afirmaba que la anonimización debía abandonarse como objetivo regulatorio, así como la tradicional distinción entre datos personales y no personales (anónimos) (Ohm, 2010, p. 1755).

Las virtudes que ofrece la seudonimización frente a la tradicional estricta anonimización son evidentes desde la perspectiva de determinados intereses notables de la sociedad, siendo un ejemplo paradigmático, al que hace referencia el propio Reglamento UE de la salud de la colectividad, ya que, al mantenerse el vínculo entre el dato y la persona, aunque sea

[17] El Instituto de Medicina de Estados Unidos sostiene que la seudonimización es un método utilizado para reemplazar las identidades verdaderas (nominativas) de individuos u organizaciones en bases de datos por pseudo-identidades (pseudo-identificaciones) que no se pueden vincular directamente a sus identidades nominativas correspondientes, siendo el beneficio de utilizar la seudonimización en la investigación en salud que al mismo tiempo que protege las identidades de los individuos, permite a los investigadores vincular los datos personales a través del tiempo y el lugar. Vid. Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 103.

extraordinariamente difícil que un tercero pueda descodificarlo, se permite no sólo ampliar los datos que se utilizan en la investigación a otros que inicialmente podían no considerarse trascendentes (ampliación de datos) sino, lo que es muy importante en el estado actual de la ciencia del Big Data, contrastar los resultados de la explotación de datos con, por ejemplo, la verdadera evolución de los pacientes (verificación de resultados)[18]. La seudonimización es, a la postre, la única garantía frente a las causalidades o correlaciones espurias que es uno de los principales riesgos del Big Data.

Como señala el Grupo Independiente de Expertos de Alto Nivel sobre IA en sus Directrices éticas para una IA fiable de 2019, el requisito de la transparencia guarda una relación estrecha con el principio de explicabilidad e incluye la transparencia de los elementos pertinentes para un sistema de IA: los datos, el sistema y los modelos de negocio. Y con el fin de posibilitar la trazabilidad y aumentar la transparencia, los conjuntos de datos y los procesos que dan lugar a la decisión del sistema de IA, incluidos los relativos a la recopilación y etiquetado de los datos así como a los algoritmos utilizados, deberían documentarse con arreglo a la norma más rigurosa posible. La trazabilidad, por tanto, facilita la auditabilidad y la explicabilidad[19]. Ello es compartido por Ohmann, Banzi, Canham, et al., cuando señalan que es recomendable compartir datos seudonimizados y no estrictamente anonimizados, debiendo ser ésta la regla general (Ohmann et al., 2017, p. 11).

El propio Reglamento UE de protección de datos hay que entender que se postula a favor de este nuevo modelo si atendemos a los términos en los que se expresa en sus artículos 6 y 9. Coincide con nuestra opinión, la profesora Vanesa Morente, la cual señala que el Reglamento recoge la posibilidad de tratar datos personales (en especial, de salud) sin la previa obtención del consentimiento cuando el tratamiento es necesario por razones de interés público y cuando el tratamiento tiene como finalidad la investigación científica (Morente Parra, 2019, pp. 26 y 27).

También ha apostado por este nuevo paradigma en la flexibilización del requisito de la anonimización, y ya desde una perspectiva estrictamente ética, el Comité Internacional de Bioética (IBC) de la UNESCO. En su Informe de 2017 sobre Big Data y Salud señala que, si bien el uso secundario de los

[18] Para el Nuffield Council, máximo órgano consultivo en materia de Bioética en el Reino Unido, la seudonimización ofrece tres ventajas en el uso secundario de los datos de salud: "to feed back information to an individual within a cohort who is discovered to be at particular risk, or to validate an analytical procedure, or to enable further data about individuals to be added over time". Vid. Nuffield Council on Bioethics, *The collection, linking and use of data in biomedical research and health care: ethical issues*, Londres, febrero 2015, p. 68.

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

datos de salud exige un nuevo consentimiento específico, tal regla encuentra una excepción cuando se implementen procedimientos técnicos adecuados que eviten que los investigadores o terceros accedan a los datos personales, como sería la seudonimización: "In case research is intended that falls outside the range of the broad consent that was obtained for the use of this data, specific consent is necessary for secondary data processing. This is an essential principle to guarantee confidentiality and data privacy. However, secondary analysis of data could be ethically admissible without a new informed consent for such secondary use provided that all the following requirements are met: 1) appropriate legal foundation; 2) evaluation by the Research Ethics Committee (REC); 3) adequate technical procedures in order to prevent researchers and third parties from accessing personal data, such as pseudo-anonymisation; 4) overriding public interest in this health research; 5) infeasible to obtain a new consent; and 6) data must have been collected according to ethical and legal requirements" (apartado 59)[20].

En similares términos, se ha expresado igualmente el Comité de Ministros del Consejo de Europa en su Recomendación CM/Rec(2019)2 sobre protección de los datos de salud, adoptada el 27 de marzo de 2019, y en la que se establece que "Where scientific research purposes allow, data should be anonymised; where research purposes do not allow this, pseudonymisation of the data – with intervention of a trusted third party at the separation stage of the identification – is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. These measures must be carried out where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects (ap. 15.9).

La Guía sobre seudonimización 1/2025 del European Data Protection Board, aprobada el 16 de enero de 2025[21], señala que el análisis de datos seudonimizados suele ser útil, ya que, en gran medida, aún se puede evaluar el contenido informativo de los datos originales. Además, la inserción de seudónimos permite vincular varios registros de datos seudonimizados relacionados con la misma persona sin necesidad de utilizar información adicional. Así pues, puede mantenerse que nos encontremos ante una garantía más, sino ante la que debiera ser considerada garantía principal en el ámbito del tratamiento de datos, y ello, porque el consentimiento se ha mostrado manifiestamente insuficiente para proteger los derechos del individuo.

Y señala la misma Guía que la seudonimización también puede ser una medida adecuada al tratar datos personales con fines de interés público, fines

[20] Vid. https://unesdoc.unesco.org/ark:/48223/pf0000248724.

[21] Vid. https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.

de investigación científica o histórica o fines estadísticos, en particular para garantizar el respeto del principio de minimización de datos.

Sí es importante recordar, en todo caso, que la seudonimización no opera autónomamente, sino que debe ir acompañada de una serie de elementos en el caso concreto que habilitan para que pueda recurrirse a la misma como garantía suficiente frente al consentimiento o la anonimización de los datos. Así, el artículo 6.4 del Reglamento UE de protección de datos establece que "Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado …", deberán tenerse en cuenta:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto[22].

Así pues, parece que se trata de una garantía que operaría, sustancialmente, en un ámbito concreto y respecto de la reutilización de los datos de salud, y ello, porque el conflicto entre la privacidad y la protección de datos y el interés colectivo en el ámbito de la salud se muestra paradójico: por un lado, se trata de datos personales especialmente protegidos por el nivel de afectación de la intimidad y privacidad del individuo, pero, por el otro, su uso masivo, sobre todo, secundario ofrece muchísimas posibilidades de avanzar en la mejora de diagnósticos y tratamientos. La explotación masiva de mis datos puede salvar la vida de otros. Y, de este modo, la seudonimización operaría como una solución proporcional entre la protección del derecho individual y el interés general, permitiendo preservar la confidencialidad de los

[22] Esta garantía se ha desarrollado normativamente, por lo que a nuestro ordenamiento jurídico interno se refiere, en el ámbito de la investigación en salud y biomédica. Así, la Disposición Adicional 17.ª de la Ley Orgánica de protección de datos, dispone que "Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial", requiriéndose el informe previo favorable del comité de ética de la investigación competente.

datos a través de la codificación compleja y, al mismo tiempo, satisfacer más adecuadamente el interés de la comunidad. Sí cabría una solución ponderada en la que la limitación al derecho individual pudiera ser capaz de superar el test de proporcionalidad. El subprincipio de proporcionalidad en sentido estricto quedaría salvaguardado a través de la seudonimización, al preservar el núcleo esencial del derecho. Un ejemplo de la importancia que el uso secundario de datos tiene en el ámbito de la salud se manifiesta cuando el Reglamento UE de protección de datos personales cita el término "salud" en 42 ocasiones, y, en varias de ellas, referido a excepciones al requisito del consentimiento informado en el caso de la reutilización de los datos de salud.

Como recuerda Barbara J Evans, en el caso de la investigación con datos de salud, no estamos enfrentando integridad física del individuo e interés colectivo, lo que más difícilmente superaría el test de proporcionalidad, y, sobre todo, el límite de la dignidad como núcleo esencial del derecho, sino la intimidad (Evans, 2018, pp. 26 y 27)[23].

Las virtudes que ofrece la seudonimización frente a la tradicional estricta anonimización son evidentes desde la perspectiva del interés de la salud de la colectividad, ya que, al mantenerse el vínculo entre el dato y la persona, aunque sea extraordinariamente difícil que un tercero pueda descodificarlo, se facilita la verificación de los resultados que nos ofrece la correlación. La seudonimización funcionaría para evitar las causalidades espurias que son uno de los principales riesgos del Big Data y, por tanto, de la IA. La indispensable verificación del proceso de desarrollo de los algoritmos exige retrotraerse a los propios datos a partir de los cuales son desarrollados. Por ello, el Reglamento UE de la IA dispone que "Para permitir la trazabilidad de los sistemas de IA de alto riesgo, verificar si cumplen los requisitos previstos en el presente Reglamento, así como vigilar su funcionamiento y llevar a cabo la vigilancia poscomercialización, resulta esencial disponer de información comprensible sobre el modo en que se han desarrollado y sobre su funcionamiento durante toda su vida útil. A tal fin, es preciso llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA de que se trate cumple los requisitos pertinentes y facilitar la vigilancia poscomercialización. Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos

[23] Esta distinción ya fue establecida hace una década por el Instituto de Medicina de Estados Unidos, señalando que habría que distinguir entre "interventional research and research that is exclusively information based". Vid. Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 3.

pertinente, elaborada de manera clara y completa. La documentación técnica debe mantenerse adecuadamente actualizada durante toda la vida útil del sistema de IA. Además, los sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de acontecimientos, mediante archivos de registro, durante toda la vida útil del sistema" (Considerando 71).

La seudonimización puede ser un instrumento, pues, muy útil para evitar la opacidad y complejidad de determinados sistemas de IA y cumplir con el deber legal de transparencia.

Sin embargo, como hemos adelantado ya antes, su virtualidad queda reducida actualmente al ámbito de los datos de salud. Y ello no debe interpretarse en el sentido de que estemos postulando ampliarlo con carácter general a cualquier tipo de datos, pero sí evaluar en qué medida, cuando concurre un interés general para la reutilización de los datos, sean o no de salud, no debe operar la seudonimización como garantía principal que satisface tanto la expectativa de privacidad del sujeto como el interés de la colectividad.

También, el modelo ha quedado algo limitado en el ámbito de la salud por obra de la nueva regulación de los datos de salud contenida en el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 –en adelante, Reglamento UE del espacio europeo de datos de salud–. En esta normativa sectorial parece volverse a una preeminencia del consentimiento del interesado frente a la seudonimización. Y así el artículo 71 consagra una suerte de derecho de autoexclusión del tratamiento de datos, en virtud del cual, el sujeto puede exigir que sus datos no sean tratados secundariamente, y ello, sin necesidad de exponer motivo alguno. El apartado 3 del precitado precepto dispone, expresamente, que "una vez que las personas físicas hayan ejercido el derecho de autoexclusión, y cuando los datos de salud electrónicos personales que les conciernan puedan identificarse en un conjunto de datos, los datos de salud electrónicos personales que conciernan a esas personas físicas no se pondrán a disposición ni se tratarán de otro modo con arreglo a permisos de datos expedidos de conformidad con el artículo 68 o a peticiones de datos de salud con arreglo al artículo 69 aprobadas después de que la persona física haya ejercido su derecho de autoexclusión".

Por tanto, el nuevo Reglamento UE opta, frente al modelo que permitiría el uso secundario de datos sin necesidad de nuevo consentimiento y a través de la garantía de la seudonimización, por una fórmula de *opt-out* similar a la que, por ejemplo, existe en el ámbito de la donación de órganos, recordando que la Ley 30/1979, de 27 de octubre, sobre extracción y trasplante de órganos, cuyo artículo 5.3 dispone que "las personas presumiblemente sanas que falleciesen en accidente o como consecuencia ulterior de éste se considerarán, asimismo, como donantes, si no consta oposición expresa del fallecido".

Ello supone, en cierto modo, como decíamos antes, una vuelta al paradigma del consentimiento informado, aunque también el Reglamento deja cierto margen de decisión a los Estados a la hora de implementar la norma, los cuales "podrán prever en su Derecho nacional un mecanismo para poner a disposición datos respecto de los cuales se haya ejercido el derecho de autoexclusión, siempre y cuando" se trate de "una medida necesaria y proporcionada en una sociedad democrática para satisfacer los fines de interés público en el ámbito de los objetivos científicos y sociales legítimos" (artículo 71.4 y 5).

Para ir concluyendo con este apartado, es importante recordar que el consentimiento no operaría como elemento legitimador del uso de los datos cuando nos encontramos ante determinadas categorías de datos, es decir, determinados datos que no pueden tratarse, pese a que mediara la autorización de tratamiento. Así, el artículo 9 del Reglamento UE de protección de datos dispone que "quedan prohibidos el tratamiento de datos personales 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 sexual de una persona física". Sin embargo, el mismo precepto añade unas excepciones a la prohibición general en el ámbito del Derecho laboral y de la seguridad y protección social, en el ámbito judicial, en el ámbito de la salud (pública, preventiva y asistencial), en el de la investigación científica o histórica o con fines estadísticos, cuando el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados, además de las excepciones generales que se derivan del artículo 6.

Por su lado, el artículo 9.1 Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, establece que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. En relación con tales datos deberían implementarse otras garantías adecuadas. El nivel y la naturaleza de estas garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos

peligrosas para los derechos fundamentales. Sin perjuicio de ello, la previsión de estas garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. La predeterminación de sus elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares (STC 76/2019, FJ 8.º).

Y es que la necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad (STC 76/2019, FJ 6.º).

Como conclusión de este apartado, puede afirmarse que los datos personales disponen de una garantía respecto de su tratamiento, el consentimiento informado que debe operar, habitualmente, de manera expresa y específica, admitiéndose, sin embargo, determinados supuestos en los que, no siendo así, sí al menos concurra una clara acción afirmativa. Y no olvidando tampoco que el derecho a la protección de datos como todo derecho o libertad no es ilimitado, pudiendo limitarse cuando concurra en conflicto con el derecho de un tercero o con el interés colectivo.

Así pues, podemos ver como apunta Luciano Floridi que existe una conexión entre la IA y la Bioética (Floridi, 2024, pp. 140 y ss), aunque ésta venga referida al campo de la salud y la biomedicina, incorporándose tanto en el campo de aquélla como en la de éstas el principio de autonomía como principio estelar, siendo la garantía legal de dicho principio el consentimiento informado. Eso sí, es importante también distinguir entre los derechos y valores en juego, dado que, en el ámbito de la IA, en lo que se refiere al uso masivo de los datos, lo que se protege a través del consentimiento es el derecho del sujeto a decidir sobre el uso de sus datos, mientras que en el ámbito de la asistencia sanitaria, el consentimiento es garantía de la integridad física del paciente. Así pues, el principio de autonomía ocupa, a través del consentimiento informado, una posición estelar en ambos ámbitos, pero garantizando diferentes derechos y valores, lo que no debe ser olvidado porque también la relevancia del objeto de protección determina una mayor o menor rigurosidad a la hora de configurarlo y exigirlo. No es lo mismo actuar sobre la privacidad del individuo que sobre su integridad física, por lo que el consentimiento en este último caso debe ser más riguroso que en el primero.

Por otro lado, también es importante tener en cuenta que el consentimiento informado del que estamos hablando es distinto del que se exige para,

en su caso, acelerar el proceso de desarrollo e introducción en el mercado de determinados sistemas de IA de alto riesgo, sin necesidad de participar en un espacio controlado de pruebas para la IA. Así, el Reglamento UE de la IA dispone que "en tales casos, teniendo en cuenta las posibles consecuencias de dichas pruebas para las personas físicas, debe garantizarse que el Reglamento establezca garantías y condiciones adecuadas y suficientes para los proveedores o proveedores potenciales. Estas garantías deben incluir, entre otras cosas, la solicitud del consentimiento informado de las personas físicas para participar en pruebas en condiciones reales". Y añade que "El consentimiento de los sujetos para participar en tales pruebas en virtud del presente Reglamento es distinto del consentimiento de los interesados para el tratamiento de sus datos personales con arreglo al Derecho pertinente en materia de protección de datos y se entiende sin perjuicio de este", siendo conveniente "prever garantías adicionales para asegurarse de que sea posible revertir efectivamente y descartar las predicciones, recomendaciones o decisiones del sistema de IA y de que los datos personales se protejan y se supriman cuando los sujetos retiren su consentimiento a participar en la prueba, sin perjuicio de sus derechos como interesados en virtud del Derecho de la Unión en materia de protección de datos" (Considerando 141).

El consentimiento informado vinculado a la IA, distinto del vinculado a la protección de datos, es definido por el Reglamento UE de la IA como "la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar" (art. 3).

Y recuerda el mismo Reglamento el problema que, en tales supuestos, plantea, "la transferencia de datos, por lo que conviene también prever que los datos recopilados y tratados a efectos de las pruebas en condiciones reales solo deben transferirse a terceros países cuando existan garantías adecuadas y aplicables con arreglo al Derecho de la Unión, en particular, de conformidad con las bases para la transferencia de datos personales previstas en el Derecho de la Unión en materia de protección de datos y, en lo referente a los datos no personales, existan garantías adecuadas con arreglo al Derecho de la Unión, como los Reglamentos (UE) 2022/868 (42) y (UE) 2023/2854 (43) del Parlamento Europeo y del Consejo" (Considerando 141).

IV. LA POSIBLE FALTA DE VIRTUALIDAD DEL MARCO DE GARANTÍAS ASENTADO, SUSTANCIALMENTE, EN EL CONSENTIMIENTO INFORMADO EN EL CONTEXTO DE LA IA

Como vamos a exponer a continuación, este modelo de garantía asentado en el consentimiento, con la excepción de la anonimización, planteó desde

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 159-200
https://doi.org/10.18543/ed.3578 • http://www.revista-estudios.deusto.es/

sus inicios problemas. Y es que como apunta Lorenzo Cotino, si bien el derecho de protección de datos personales ha girado estructuralmente en el consentimiento del titular de los datos personales, ello ha quebrado hace tiempo. Las razones de tal quiebra derivan, esencialmente, de que la sociedad no está dispuesta a renunciar al uso de las IT y no tiene una fuerte cultura de la privacidad, lo que lleva a hacer casi irreal o inefectiva la garantía del consentimiento. Éste, en la práctica, "viene masivamente por defecto". Por ello, "no es realista en modo alguno creer que existe un efectivo control de la información personal a través del consentimiento y los derechos que lo complementan. El consentimiento se torna en una carta blanca al descontrol del flujo de los datos personales. El consentimiento acaba configurándose como un simbolismo que conlleva, a la postre, al fracaso de la privacidad pretendida y a la inoperancia del sistema de protección" (Cotino Hueso, 2017, p. 145).

Es lo que se ha denominado, en el ámbito de la protección de datos, el estándar subjetivo del consentimiento que lo analiza desde la perspectiva de aquél que debe prestarlo, y hace referencia al hecho de si un interesado particular es capaz de ejercer su expresión de voluntad autónoma en el contexto específico. Como señala Elena Gil, "en ocasiones, a pesar de que los requisitos formales del consentimiento se respeten, sobre el interesado actúan otros factores que cuestionan la confiabilidad en la manifestación de aquiescencia. Así, en muchas ocasiones puede cumplirse con la función formal pero no material del consentimiento" (Gil González, 2020, p. 156).

Y es que el estado de la técnica actual, caracterizado por prácticas más extendidas, intensivas e impredecibles ha modificado el valor real del consentimiento del interesado. Por ello, como venimos manteniendo, el consentimiento ha mostrado deficiencias, que se agudizan en entornos Big Data que son los que nutren a la IA.

Por otro lado, debe recordarse que la relación entre el presunto cedente de los datos y el cesionario no es siempre o, incluso, habitualmente, una relación caracterizada por la igualdad entre las partes, existiendo una posición de poder o dominio del último. El propio Reglamento UE de protección de datos recuerda en su Considerando 43 que para garantizar que el consentimiento se ha dado libremente, éste no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Y el Reglamento presume que ello ocurre cuando no se permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la

prestación de un servicio, sea dependiente del consentimiento, aún cuando éste no sea necesario para dicho cumplimiento.

El propio Tribunal Constitucional en su Sentencia 27/2020, relativa al uso de una imagen fotográfica de un individuo por un medio de comunicación como soporte gráfico de una noticia de sucesos, el cual mantenía que la imagen era pública, no siendo necesario, pues, el consentimiento informado, al haber sido incluida voluntariamente en una red social (Facebook), recuerda que "el aumento de popularidad de las redes sociales ha transcurrido en paralelo al incremento de los niveles de intercambio de contenidos a través de la red. De este modo, los usuarios han pasado de una etapa en la que eran considerados meros consumidores de contenidos creados por terceros, a otra –la actual– en la que los contenidos son producidos por ellos mismos. Con plataformas como Facebook, Twitter, Instagram o Tuenti, por citar solo algunas, los usuarios (porque jurídicamente ostentan tal condición) se han convertido en sujetos colaborativos, ciudadanos que interactúan y que ponen en común en redes de confianza lo que tienen, lo que saben o lo que hacen, y que comparten con un grupo más o menos numeroso de destinatarios –usuarios igualmente de la redes sociales en Internet– todo tipo de imágenes, información, datos y opiniones, ya sean propios o ajenos".

Y añade a continuación que "contemplado de esta manera el panorama tecnológico actual y aceptando que la aparición de las redes sociales ha cambiado el modo en el que las personas se socializan, hemos de advertir sin embargo –por obvio que ello resulte– que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica. Por consiguiente, salvo excepciones tasadas, por más que los ciudadanos compartan voluntariamente en la red datos de carácter personal, continúan poseyendo su esfera privada que debe permanecer al margen de los millones de usuarios de las redes sociales en Internet, siempre que no hayan prestado su consentimiento de una manera inequívoca para ser observados o para que se utilice y publique su imagen".

Para el Tribunal, "el entorno digital no es equiparable al concepto de "lugar público" del que habla la Ley Orgánica 1/1982, ni puede afirmarse que los ciudadanos de la sociedad digital hayan perdido o renunciado a los derechos protegidos en el art. 18 CE", por lo que "debemos seguir partiendo del mismo principio básico que rige el entorno analógico y afirmar que el reconocimiento constitucional de los derechos fundamentales comprendidos en el art. 18 CE conlleva la potestad de la persona de controlar los datos que circulan en la red social y que le conciernen", debiendo concurrir "una autorización inequívoca para la captación, reproducción o publicación de la imagen por parte de su titular".

Y dado el contexto en el que suele prestarse el consentimiento en el marco de dichas redes sociales, el Tribunal considera que "no puede reputarse como

consentimiento indefinido y vinculante aquel que se prestó inicialmente para una ocasión o con una finalidad determinada", ya que "de conformidad con el comportamiento usual de los usuarios en las redes sociales en Internet, y especialmente en aquellas como Facebook, no puede afirmarse que don I.I.L. con la publicación de una fotografía suya en su perfil estuviera creando en la editora demandante de amparo (o cualquier otro medio de prensa) la confianza de que autorizaba su reproducción en el periódico como víctima de un suceso".

Y es que "las denominadas "condiciones de servicio" incluidas en la "Declaración de derechos y responsabilidades" que necesariamente deben aceptar los usuarios de Facebook para poder utilizar la red revelan que el contrato suscrito por ambas partes es típicamente de los llamados de "adhesión", con la particularidad de que se formaliza mediante un clic en el botón de la aplicación digital previsto al efecto. Es decir, estamos en presencia de un contracto electrónico puro. El uso de condiciones generales empleado en este procedimiento de contratación online, sus características, y la falta de capacidad de los usuarios/consumidores para negociar el clausulado, arroja dudas relevantes sobre la existencia de una adecuada manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta indiscriminadamente el tratamiento de su imagen por cualquier tercero que pueda tener acceso a ella. Los avisos legales, las condiciones de uso y las políticas de privacidad están redactadas en un lenguaje generalista, de difícil comprensión para el usuario medio, de tal suerte que, a pesar de encontrarse recogidas en el sitio web, no alcanzan su finalidad última, que no es otra que la comprensión por el usuario del objeto, la finalidad y el plazo para el que otorga dicha autorización. A ello hay que añadir que en dicha red social aparece activado por defecto el mayor grado de publicidad, en contraste con el hecho de que el perfil de acceso completamente público supone un grave riesgo para la seguridad de los datos personales de los usuarios, en la medida en que estos serán accesibles por parte de cualquier usuario de la plataforma".

Para el Alto Tribunal, "la información ofrecida en la red social está inmersa en una maraña de cláusulas contractuales contenidas en un prolijo y extenso documento alojadas en lugares del sitio web de difícil acceso para el usuario, reservándose, por otro lado, la plataforma la posibilidad de modificar las condiciones de uso y privacidad en cualquier momento, sin necesidad de preaviso a los usuarios registrados que con anterioridad las hubieran aceptado. Por tanto, hay que concluir que el ciudadano desconoce la mayor parte de las veces el contenido real y las consecuencias del otorgamiento de la autorización exigida para su registro y utilización, pues resultan de no fácil comprensión para cualquier usuario medio que no disponga de conocimientos jurídicos y tecnológicos, por lo que difícilmente en este caso puede hablarse de un consentimiento basado en información fiable o confiable".

A lo dicho por nuestro Tribunal Constitucional habría que añadir que, plantear la validez de un consentimiento como el mencionado en dicho caso, supone tanto como permitir que el sujeto quede expuesto a la exclusión social, partiendo de que, guste o no, las relaciones sociales operan en gran parte a través de tales redes sociales. No es erróneo ni exagerado afirmar que los titulares de datos no reparan en los términos en que se otorga el consentimiento ni su trascendencia individual y colectiva.

El sujeto presta el consentimiento para el tratamiento no por razones directamente vinculadas a lo que se le pide, sino para poder estar o permanecer en la relación social que supone la red, para poder estar informado de la actualidad o para acceder al servicio que necesita. Y es que no debe olvidarse, por otra parte, que el consentimiento al tratamiento de datos sirve también como instrumento de pago en manos del consumidor (en su doble condición de consumidor y titular de sus propios datos personales) para disfrutar de ciertos bienes y servicios en el entorno digital (Castillo Parrilla, 2023, p. 69).

Castillo Parrilla ha afirmado con razón que "el consentimiento informado es la base de legitimación más cómoda y que mayor nivel de seguridad jurídica ofrece desde la perspectiva del responsable del tratamiento de los datos, ya que necesita menor profundidad de estudio y resulta más fácilmente adaptable a cada caso. No menos importante es la (apariencia de) protección de la autonomía individual del interesado que esta base de legitimación genera" (Castillo Parrilla, 2023, p. 68).

En palabras de Eva Gil y Antonio Troncoso, el consentimiento parte de que la persona ha leído la información que se le presenta, la comprende y toma una decisión, lo que sólo se cumple en entornos comprensibles y previsibles. Sin embargo, el consentimiento no funciona bien en entornos cambiantes y complejos, como es el Big Data. En estos ámbitos, el consentimiento se convierte en algo automático e irreflexivo. Además, la regla del consentimiento supone responsabilizar a la persona por la toma de decisiones para las que no está preparada, de forma que al final el consentimiento se vuelve en su contra. Y, por ello, consideran que no hace falta aferrarse al consentimiento como salvoconducto único (Gil González, 2020; y Troncoso Reigada, 2024, p. 487).

Por lo que se refiere a la anonimización, el problema radica en determinar en qué medida ello es realmente posible, es decir, que no pueda establecerse a través de la IA la correlación entre los datos y la persona. Se parte ya de la premisa de que cada vez es más sencillo reidentificar datos previamente anonimizados, e incluso identificar o inferir características de personas a partir de datos anónimos o de perfiles abstractos que no se han nutrido de datos de dichas personas (Castillo Parrilla, 2023, p. 64). El propio desarrollo de la AI ayuda a ello.

V. OTRAS PROPUESTAS PARA LA PROTECCIÓN DE LOS DATOS EN EL CONTEXTO DE LA IA

Como hemos expuesto en el apartado anterior, el consentimiento informado no ha operado como una garantía robusta del derecho a la protección de datos, antes al contrario. Por ello, se propone, frente a la garantía del consentimiento, reforzar las obligaciones legales preventivas de privacidad en el diseño y por defecto y de la evaluación de impacto de protección de datos.

Se ha propuesto una suerte de metáfora, de manera que por medio ambiente tecnológico contaminado debe entenderse aquel en el que la ingente cantidad de datos y la potencia de las herramientas de analítica de *big data* no permiten a los individuos desenvolverse en el entorno digital con unas mínimas expectativas de anonimato que garanticen el libre desarrollo de su personalidad (Castillo Parrilla, 2023, p. 64).

Y todo ello sobre la base de tres acciones fundamentales en mejora de una efectiva protección del derecho:

1. Reducir la «emisión de consentimientos» al tratamiento de datos personales durante la fase de recolección de datos.
2. Controlar los estándares de calidad de los datos durante la fase de construcción del modelo (perfil abstracto); teniendo en cuenta la importancia de prevenir los sesgos como criterio de calidad (fases de recolección de datos y de construcción del modelo).
3. Subrayar la necesidad de una aplicación integral del RGPD a toda actividad de tratamiento de datos, tanto la consistente en utilizar los datos (personales o no) para durante el desarrollo del modelo como aquella para la posterior aplicación de perfiles a personas concretas durante la fase de implementación del modelo (Castillo Parrilla, 2023, pp. 67 y 68).

Por otro lado, se ha planteado también la oportunidad de trascender a una visión esencialmente individual del derecho a la protección de datos: la privacidad de grupo.

El derecho a la protección de datos ha tenido como eje central el individuo y no tanto a la colectividad. Y tal visión no solo ha impedido un uso de los datos en garantía del interés colectivo, primando la dimensión subjetiva del derecho, pese a que pudiera superarse el test de proporcionalidad, sino que ha acabo por desproteger al propio derecho al fundamentar la garantía de su eficacia en la figura del consentimiento informado. La visión individual del derecho ni ha atendido al interés general que el Big Data puede satisfacer, ni ha protegido realmente al derecho.

Por ello, Castillo Parrilla "propone promover una dimensión colectiva a este derecho, en la medida en que se han generado nuevos riesgos que afectan

a la sociedad en su conjunto que ya no pueden resolverse *ex post* y de manera reactiva" (Castillo Parrilla, 2023, pp. 59 y 63). Sería una fórmula similar a la seguida desde hace décadas en el ámbito del derecho al medioambiente.

La propuesta es eminentemente práctica, más que ontológica. Ya el Comité de Bioética de España nos recordó en uno de sus informes que la autonomía se ha interpretado en clave meramente individual, como exigencia ética de respetar los deseos del individuo al margen de su condición de miembro de una comunidad en la que convive y se desarrolla, no toma suficientemente en cuenta el entramado de vínculos que atraviesan las posibilidades cognitivas y volitivas de la persona y que le ligan con su entorno. La autonomía se construye con elementos que relacionan al sujeto con otros, así como con escenarios sociales y perspectivas culturales. Por ello, atender a todos estos aspectos que configuran la autonomía no solo con la capacidad racional sino también, en un sentido más amplio y comprensivo, como capacidad relacional, permite una aproximación más certera al tipo de situaciones con las que se enfrenta la persona cuando toma decisiones. Porque, lo valioso no es ser autónomo en un sentido restringido de razonamiento guiado por un ideal de independencia, sino en un sentido amplio de capacidad relacional o referencial para la toma de decisiones. La determinación de qué somos capaces se produce necesariamente en contextos compartidos con otros y tiene un significado de contraste, se lleva cabo en relación y como respuesta a determinaciones que se han adoptado en el medio social y cultural[24].

VI. LA ALFABETIZACIÓN DIGITAL COMO GRAN RETO

Como hemos comprobado a lo largo de nuestro trabajo, el Derecho tiene mucho que ofrecer para salvaguardar nuestros derechos y libertades frente a los usos inadecuados de la IA y, en concreto, para preservar nuestra privacidad y la confidencialidad de nuestros datos personales. Sin embargo, el principio ético-legal en el que se han fundamentado las necesarias garantías, la autonomía, siendo el consentimiento informado su instrumento de protección no parece que realmente esté cumpliendo satisfactoriamente su cometido.

La digitalización no es neutra. Su propósito no ha sido solo el de ofrecer de manera más accesible datos y servicios, sino que ello se ha hecho con el principal propósito de obtener nuestros datos para poder proceder a su uso masivo y a desarrollar los algoritmos que hagan viable la IA. Este propósito ha generado o, mejor dicho, institucionalizado una cultura de la renuncia a la

[24] Puede accederse a dicho Informe a través del siguiente enlace: http://assets.comitedebioetica.es/files/documentacion/Informe%20CBE%20final%20vida%20y%20la%20atencion%20en%20el%20proceso%20de%20morir.pdf.

privacidad para poder acceder a los datos y servicios o para, como ocurre con las redes sociales, no quedar al margen del grupo o de la colectividad. Y una sociedad de consumo como la nuestra, en la que los deseos pueden cumplirse inmediatamente a golpe de teclado lo ha acrecentado.

En palabras de Francisco Balaguer, "la escasa preocupación de los nativos digitales por su derecho a la intimidad se explica en gran medida porque han sido "dopados" muy tempranamente por las compañías tecnológicas, con aplicaciones que están destinadas justamente a la exhibición pública y a la búsqueda de reconocimiento a través del uso de las redes sociales. Su cultura no tiene nada que ver con la de la Constitución sino con una visión mercantil de sus propios derechos que se activa solamente cuando consideran que el producto que reciben es deficitario" (Balaguer Callejón, 2022, p. 46). El principal problema es, nos dice Vázquez-Pastor Jiménez, "cómo proteger a quien voluntariamente desvela su intimidad en la red. En efecto, los menores no identifican realmente los riesgos que suponen las redes sociales para su privacidad y otorgan voluntariamente su consentimiento para adherirse a ellas. Este consentimiento tiene un papel fundamental en los distintos usos que se dé a sus datos en el entorno online" (Vázquez-Pastor Jiménez, 2022, p. 1120).

Los derechos se protegen ahora desde la posición de los consumidores. Se trata de "facultades instrumentales de los derechos económicos y se garantizan solamente desde la lógica económica. Ya no conectan directamente con la dignidad sino con la inserción del individuo como una pieza más dentro del contexto económico" (Balaguer Callejón, 2022, p. 115).

También, como recuerda la Oficina C en su reciente Informe sobre redes sociales y menores de 2025[25], las personas menores en nuestro país acceden de forma cotidiana a redes sociales desde edades cada vez más tempranas, incluso antes de la edad mínima de acceso sin consentimiento paterno mediante autodeclaraciones y sin sistemas de verificación de edad efectivos. Según datos de UNICEF más del 90 por ciento de los menores con once años de edad están a esa edad en, al menos, una red social[26].

Para la Oficina C, en el mismo Informe ya citado, la edad mínima de catorce años para acceder a las redes de forma independiente responde más a criterios puramente legales derivados de la regulación de la protección de

[25] Puede accederse a dicho Informe a través de la página web de la Oficina C en el siguiente enlace: https://www.oficinac.es/sites/default/files/informes/2025_10_30_InformeC-Redes-sociales-menores_oficinac-fecyt-congreso.pdf.

[26] UNICEF, Impacto de la tecnología en la adolescencia. Un estudio comprensivo e inclusivo hacia el uso saludable de las TRIC, 2021. Puede accederse a dicho trabajo a través del siguiente enlace: https://www.unicef.es/sites/unicef.es/files/comunicacion/Informe_estatal_impacto-tecnologia-adolescencia.pdf.

datos como de la capacidad del menor para firmar contratos, sin implicar realmente un uso seguro por su parte. Su falta de alfabetización digital y mediática, junto con la inmadurez para modular su uso, los hace especialmente vulnerables, más aún, cuando muchas plataformas emplean patrones de diseño persuasivo, basados en principios de la psicología del comportamiento y la economía conductual con el fin de influir más fácilmente en el comportamiento de los usuarios, explotando sesgos cognitivos y vulnerabilidades emocionales y activando circuitos neurales de recompensa mediante distintos elementos de su diseño. Además, los perfiles digitales de niños, niñas y adolescentes son altamente valiosos para las plataformas.

Por ello, considerar que la mejor garantía para afrontar ética y legalmente los retos que nos trae la IA y, en especial, como hemos tratado en este trabajo, para salvaguardar la dignidad, la privacidad y el uso indebido de datos personales sigue siendo el consentimiento informado supone un verdadero autoengaño. No estamos proponiendo, obviamente, excluir del sistema la operatividad de éste, sino evitar caer en el error de considerar que normativizándolo y adaptándolo a estos nuevos retos de la IA resolveremos, en gran parte, los problemas que surgen en relación con nuestros derechos y libertades. Estamos proponiendo, pues, incorporar no solo un enfoque legal o normativo, sino también formativo.

Ya antes hemos recogido alguna de las nuevas fórmulas o propuestas que se ofrecen, añadiendo ahora, a modo de conclusión, la última de ellas: la alfabetización digital.

Y es que resulta harto difícil tratar de imponer la cultura de la privacidad y de la protección de datos personales a través del consentimiento cuando la propia sociedad ha renunciado a ello, no como concepto general o temor social frente a la IA, sino como actitud o conducta diaria.

Y, por ello, parece que el camino es tratar de recuperar o, incluso, crear una nueva cultura que, sin menoscabo de los avances positivos del Big Data y la IA, nos haga conscientes de los valores que están en juego. Habría que construir una narrativa alternativa a la economicista y tecnológica, defendiendo el pluralismo y los valores que han hecho del constitucionalismo y sus derechos y libertades un factor esencial del progreso (Balaguer Callejón, 2022, p. 189).

Como comenta Arias Maldonado, si la imprenta convirtió a todos en lectores potenciales y ello exigió una adaptación de los ciudadanos, la Red nos convierte a todos en transmisores y receptores de información y exige igualmente un periodo de aprendizaje (Arias Maldonado, 2024, pp. 208 y 209), una nueva etapa de alfabetización.

La propuesta de la alfabetización ya la hemos hecho en el entorno del debate frente al anticientifismo que tan de la mano va con los nuevos populismos y con los nuevos enemigos de la democracia constitucional nacida

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 159-200
https://doi.org/10.18543/ed.3578 • http://www.revista-estudios.deusto.es/

tras las experiencias de finales de la primera mitad del siglo XX (de Montalvo Jääskeläinen, 2023). También se ha formulado en relación con la IA por autores de prestigio y grandes conocedores de este nuevo contexto como Paolo Benanti. Este nos dice en su análisis de la "era digital" que existe una necesidad urgente de educación mediática (Benanti, 2024, p. 116), como transmisión de los conocimientos necesarios para manejar adecuadamente las nuevas tecnologías, no desde una perspectiva tecnológica, las denominadas skills o habilidades en nuestra lengua, sino desde la de los valores y rasgos esenciales de la sociedad y de la persona en juego. Es decir, luchar contra, permítasenos la expresión, el analfabetismo de los derechos y las libertades en la era de la IA.

En palabras de Nicolás Marín, "la nueva alfabetización tiene dos planos, uno meramente técnico y otro de carácter psicológico y moral y ambos se aprenden y se entrenan en las diversas instituciones educativas con que cuenta la sociedad. Esta dimensión educativa es fundamental para conseguir personas críticas ante la evolución de la sociedad en general y ante el fenómeno de la posverdad en particular. Es la batalla contra el analfabetismo digital, puesto que una sociedad de analfabetos es fácilmente manipulable" (Nicolás Marín, 2019, p. 333).

La UNESCO la ha definido como la capacidad de acceder, gestionar, comprender, integrar, comunicar, evaluar y crear informaciones mediante la utilización segura y pertinente de las tecnologías digitales para el empleo, un trabajo decente y la iniciativa empresarial. Esto incluye competencias como la alfabetización informática, la alfabetización en las TIC, la alfabetización informativa y la educación mediática, que tienen como objetivo empoderar a las personas y, en particular, a los jóvenes, para que adopten una actitud crítica en cuanto a la utilización de las tecnologías de la información y las tecnologías digitales, y para que puedan desarrollar su resiliencia frente a la desinformación, el discurso de odio y el extremismo violento[27].

Para la Oficina C en su reciente Informe ya citado de 2025, la generación de conciencia social sobre los riesgos del ecosistema digital es clave para que las personas puedan identificarlos, ya que, para poder actuar con autonomía en los entornos digitales, se requieren competencias específicas que no se adquieren solo por interactuar con la tecnología.

La propuesta de alfabetización no aparece mencionada explícitamente en el Reglamento UE de protección de datos, pero sí en el de la IA, el cual dispone, literalmente que "Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, la alfabetización

[27] Vid. https://www.unesco.org/es/literacy/need-know#:~:text=La%20UNESCO%20define%20la%20alfabetización,decente%20y%20la%20iniciativa%20empresarial.

en materia de IA debe dotar a los proveedores, responsables del despliegue y personas afectadas de los conceptos necesarios para tomar decisiones con conocimiento de causa en relación con los sistemas de IA", añadiendo, a continuación, que "En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución. Además, la puesta en práctica general de medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, sostener la consolidación y la senda de innovación de una IA fiable en la Unión. El Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA») debe apoyar a la Comisión para promover las herramientas de alfabetización en materia de IA, la sensibilización pública y la comprensión de los beneficios, los riesgos, las salvaguardias, los derechos y las obligaciones en relación con el uso de sistemas de IA. En cooperación con las partes interesadas pertinentes, la Comisión y los Estados miembros deben facilitar la elaboración de códigos de conducta voluntarios para promover la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el manejo y el uso de la IA" (Considerando 20).

Y su artículo 3 define alfabetización digital o en materia de IA en los siguientes términos: "«alfabetización en materia de IA»: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar"[28].

Por tanto, alfabetizar es transmitir conocimiento de causa.

Y el concepto sigue siendo mencionado por el citado Reglamento más adelante: "El despliegue de sistemas de IA en el ámbito educativo es importante para fomentar una educación y formación digitales de alta calidad y para que todos los estudiantes y profesores puedan adquirir y compartir las

[28] Y vuelve a referirse al concepto el artículo 4 del mismo Reglamento: "Alfabetización en materia de IA. Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas".

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 74/1, enero-junio 2026, págs. 159-200
https://doi.org/10.18543/ed.3578 • http://www.revista-estudios.deusto.es/

capacidades y competencias digitales necesarias, incluidos la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos" (Considerando 56).

Recoge, también, una mención expresa a la alfabetización el Reglamento UE del espacio europeo de datos de salud: "Mejorar la alfabetización sanitaria digital de las personas físicas y de los profesionales sanitarios es esencial para la confianza y la seguridad y el uso adecuado de los datos de salud y, por ende, lograr una aplicación satisfactoria del presente Reglamento".

Y ello, porque "la mejora de la alfabetización sanitaria digital es fundamental para facultar a las personas físicas para que ejerzan un verdadero control sobre sus datos de salud, gestionen activamente su salud y su asistencia, y entiendan las implicaciones de la gestión de tales datos para un uso tanto primario como secundario. Los diferentes grupos demográficos tienen distintos grados de alfabetización digital, lo que puede afectar a la capacidad de las personas físicas para ejercer los derechos de control de sus datos de salud electrónicos".

Y añade que este proceso de alfabetización debe "prestarse especial atención a las personas con discapacidad y a los grupos vulnerables, incluidas las personas migrantes y las de edad avanzada" (Considerando 89).

Más adelante, en el artículo 84 el mismo Reglamento regula dicha alfabetización, estableciendo que "los Estados miembros promoverán y apoyarán la alfabetización en materia de salud digital y el desarrollo de las competencias y capacidades pertinentes para los pacientes. La Comisión apoyará a los Estados miembros a este respecto. Las campañas o programas de sensibilización tendrán por objeto, en particular, informar a los pacientes y al público en general sobre uso primario y secundario en el marco del EEDS, incluidos los derechos que se derivan de él, así como las ventajas, los riesgos y los posibles beneficios del uso primario y secundario para la ciencia y la sociedad".

¿Y cómo articular esta alfabetización?

Obviamente, no es tarea fácil. Además, según recuerda la Oficina C, la evidencia empírica sobre su efectividad en población joven aún es limitada, aunque se reconoce que, si bien no reduce necesariamente la exposición a riesgos, sí contribuye a mitigar sus efectos negativos y fortalece la resiliencia digital, ya que los adolescentes con mayor alfabetización digital tienden a gestionar mejor las consecuencias de sus experiencias en línea y adoptan estrategias más eficaces para proteger su bienestar.

Además, ya tenemos modelos en algunos países de nuestro entorno europeo, como Finlandia, Dinamarca, Estonia, Suecia e Irlanda, en un ámbito directamente conectado al que venimos abordando como es el de la alfabetización mediática. Por ejemplo, en Finlandia esta alfabetización se ha implantado en el sistema educativo con carácter transversal, no configurándose una asignatura concreta como tal, sino incorporándose diferentes contenidos en

todas las asignaturas. Se da libertad a los maestros para que adapten el modelo oficial propuesto a sus diferentes materias profesores tienen libertad prácticamente absoluta para adaptar las recomendaciones educativas del Gobierno como consideren más adecuado para conseguir los fines de dicha política pública[29]. Así, los alumnos finlandeses aprenden, desde los seis años, a leer las fuentes informativas de manera crítica, a evaluar y verificar los sitios web, a encontrar las fuentes para saber si una noticia dudosa es verídica o no, o a comprobar lo fácil que es manipular las estadísticas. El objetivo es dotar a los individuos de instrumentos para protegerse frente a los nuevos escenarios de amenaza social, como son la difusión sistemática y selectiva de desinformación, los mensajes antidemocráticos, la creciente frecuencia de los discursos de odio y el acoso sexual mediado, así como las violaciones de la privacidad y la seguridad de los datos. Se persigue, así, inculcar en los ciudadanos, desde muy jóvenes, un interés por el aprendizaje independiente[30]. Y este aprendizaje independiente permite recuperar la conciencia sobre la importancia de la intimidad y privacidad para el individuo.

Así pues, como decíamos, la tarea no es sencilla, pero tampoco imposible. Eso sí, entendemos que en el contexto de desatención hacia la privacidad en el que están desarrollándose las nuevas tecnologías, promoverlo es ineludible y mucho más eficaz que la mera aprobación de normas y garantías específicas.

Y acabamos ya. Como dijera el Papa Francisco, no vivimos una época de cambios, sino un verdadero cambio de época[31], y ello, en palabras ahora de Paolo Benanti supone que concurren dos fenómenos: el agotamiento de un modelo cultural preexistente con su contenido de creencias sobre la realidad y el hombre, y la aparición de una nueva forma de explicar la realidad y lo humano (Benanti, 2024, p. 30).

Pues bien, que este cambio de época no nos haga olvidar el valor que ostentan para la paz y convivencia de la sociedad los derechos y libertades.

Y empezábamos nuestro texto con un filósofo poeta, Byung-Chul Han y lo concluimos con un poeta filósofo, José Luis Borges, quien escribiera en su breve poema titulado "Eternidades", incluido en su obra *La rosa profunda* que

> *"Solo perduran en el tiempo las cosas*
> *Que no fueron de este tiempo"*

[29] Vid. https://www.epe.es/es/internacional/20221202/guardian-finlandes-anti-fake-news-ninos-manipulacion-79274554.

[30] Vid. https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

[31] Discurso del Papa Francisco a la Curia Romana en ocasión de la presentación de las felicitaciones navideñas. 21 diciembre 2019. Puede accederse al discurso a través del siguiente enlace: https://www.vatican.va/content/francesco/es/speeches/2019/december/documents/papa-francesco_20191221_curia-romana.html.

Y es que los derechos y libertades no pertenecen a un tiempo que pasó, sino que perduran como lo hace el ser humano y su dignidad.

VII. BIBLIOGRAFÍA

Alcalde Bezhold, G. y Alfonso Farnós, I., "Utilización de tecnología Big Data en investigación clínica", *Rev Der Gen H*, núm. Extraord., año 2019, pp. 55 a 83.

Al Hasani Maturano, A., *El impacto de la inteligencia artificial y los derechos fundamentales, Aranzadi*, Cizur Menor, 2024.

Alós, F. y Puig-Ribera, A., "Uso de wearables y aplicaciones móviles (mHealth) para cambiar los estilos de vida desde la práctica clínica en Atención Primaria: una revisión narrativa", *Atención Primaria Práctica*, vol. 3, núm. S1, año 2021, pp. 1 a 5.

Arias Maldonado, M., *(Pos)verdad y democracia*, Página Indómita, Barcelona, 2024.

Balaguer Callejón, F., *La Constitución del algoritmo*, Fundación Manuel Giménez Abad, Zaragoza, 2022.

Benanti, P., *La era digital. Teoría del cambio de época: persona, familia y sociedad*, Encuentro, Madrid, 2024.

Castillo Parrilla, J.A., "Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la Inteligencia Artificial", *Derecho Privado y Constitución*, núm. 43, julio-diciembre 2023, pp. 53 a 88.

Cotino Hueso, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, año 9 (2017), núm. 24, pp. 131 a 150.

Cotino Hueso, L., "Una regulación legal y de calidad para los análisis automatizados de datos o con Inteligencia Artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 63, año 2023, pp. 1 a 22.

de Montalvo Jääskeläinen, F., "¿Cabe limitar en nuestro ordenamiento constitucional el discurso anticientifista?: anticientifismo y libertad de divulgación científica", Rivista Associazione Italiana dei Costituzionalisti, núm. 4, año 2023, pp. 399 a 439.

Evans, B. J., "Big Data and Individual Responsability", en Glenn Cohen, I., Fernández Lynch, H., Vayena, E. y Gasser, U. (Edit.), *Big Data, Health Law and Bioethics,* Cambridge University Press, Cambridge, 2018.

Floridi, L., *Ética de la inteligencia artificial,* Herder, Barcelona, 2024.

Gil González, E., *El interés legítimo en el tratamiento de datos personales masivos*, tesis doctoral, Universidad CEU San Pablo, Madrid, 2020.

Morente Parra, V., "Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", *Revista Derechos y Libertades,* número 41, época II, julio 2019, pp. 225 a 260.

Nicolás Marín, J. A., "Posverdad: cartografía de un fenómeno complejo", *Diálogo Filosófico*, núm. 105, año 2019, pp. 302 a 340.

Ohm, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, núm. 57, año 2010, pp. 1 a 64.

Ohmann, C., Banzi, R., Canham, S. et al., "Sharing and reuse of individual participant data from clinical trials: principles and recommendations", *BMJ Open,* 7, 2017, pp. 1 a 24.

Pérez-Ugena, M., "La Inteligencia Artificial: definición, regulación y riesgos para los derechos fundamentales", *Estudios de Deusto*, *Revista de Derecho Público*, Vol. 72/1 enero-junio 2024, pp. 307 a 337.

Romana García, M.L. y Hernández Pardo, B., "Protección de datos: La "seudonimización" inexistente", *Derecho y Salud*, vol. 28, núm. 1, 2018, pp. 92 a 103.

Troncoso Reigada, A., "Algunos debates dogmáticos sobre el derecho fundamental a la protección de datos personales", en Balaguer Callejón, F., Vidal Prado, C. y Elías Méndez, C. (Coords.), *Estudios sobre Derecho constitucional español, comparado y europeo. Liber Amicorum Yolanda Gómez Sánchez*, Centro de Estudios Políticos y Constitucionales, Madrid, 2024.

Vázquez-Pastor Jiménez, L., "Los derechos de la personalidad del menor de edad en la era digital. La dicotomía entre autonomía y protección", Actualidad Jurídica Iberoamericana, núm. 17, año 2022, pp. 1112 a 1153.